MASTER'S THESIS

Symbolische versus substantiële omgang met de GDPR; de invloed van saillante stakeholders.

Brandsma, R. (Rimmert)

Award date:
2020

Symbolische versus substantiële omgang met de GDPR; de invloed van saillante stakeholders.

Opleiding:	Open Universiteit, faculteit Management, Science & Technology Masteropleiding Business Process Management & IT
Cursus:	IM9806 Afstudeertraject Business Process Management and IT
Student:	ing. Rimmert Brandsma
Identiteitsnummer:	
Datum:	16-06-2020
Afstudeerbegeleider	dr. Laury Bollen
Meelezer	dr. Rachelle Bosua
Versie nummer:	AF 0.4
Status:	definitief

Abstract

In dit onderzoek is het effect bestudeerd van Stakeholder Salience i.r.t. Data Protection op de symbolische versus substantiële omgang met de GDPR. Hierbij zijn openbare publicaties uit 2018 van 107 Europese beursgenoteerde ondernemingen m.b.v. een content analyse onderzocht. Belangrijkste resultaat van dit onderzoek is dat een hoge (c.q. lage) prioriteit die stakeholders geven aan Data Protection (in de perceptie van de organisatie) resulteert in een meer substantiële (c.q. meer symbolische) omgang met de GDPR. Dit effect wordt versterkt door de beschikbare middelen van een organisatie.

Sleutelbegrippen

Stakeholder Salience, symbolic versus substantive legitimation, GDPR, CSR disclosure, GRI, Materiality Matrix

Samenvatting

In dit onderzoek is de omgang van organisaties met de General Data Protection Regulation (GDPR) of de Algemene Verordening Gegevensbescherming (AVG) bestudeerd. Aangezien de GDPR hiervoor geen duidelijke richtlijnen geeft, moeten organisaties zelf besluiten hoe zij de GDPR implementeren en hoe zij voldoen aan de GDPR. In dit onderzoek is concreet bestudeerd wat het effect is van de mate van saillantie van stakeholders i.r.t. Data Protection op een meer symbolische c.q. meer substantiële omgang met de GDPR. De saillantie van stakeholders (Stakeholder Salience) wordt bepaald door de mate waarin stakeholders – in de perceptie van de managers van een organisatie – prioriteit geven aan in dit geval Data Protection. Hiertoe zijn m.b.v. een contentanalyse de jaarverslagen en eventuele Corporate Social Responsibility (CSR) rapportages, privacy statements en codes of conduct uit 2018 onderzocht van 107 Europese ondernemingen, die genoteerd zijn aan de hoofdbeurzen van Amsterdam, Brussel, Parijs, Frankfurt, Dublin en Milaan. Stakeholder Salience is hierbij afgeleid van de gegevens uit de materialiteitsmatrices, die deze ondernemingen hebben gepubliceerd als onderdeel van de Global Reporting Initiative (GRI) richtlijnen, die door deze ondernemingen worden toegepast. Hoe hoger (lager) de prioriteitsscore in de matrix, hoe hoger (lager) de saillantie. Stakeholder Salience is in dit onderzoek niet alleen in absolute zin (als afzonderlijke prioriteit), maar ook in relatieve zin (als gewogen prioriteit t.o.v. andere prioriteiten) gemeten. Managers moeten immers tegelijkertijd rekening houden met verschillende stakeholders en met de verschillende aanspraken die stakeholders op de organisatie maken. De omgang met de GDPR is afgeleid uit het aantal GDPR gerelateerde maatregelen dat een organisatie heeft beschreven in de openbare publicaties. Hierbij is getoetst op 24 verschillende maatregelen, die betrekking hebben op verschillende GDPR artikelen. Hoe meer (minder) GDPR gerelateerde maatregelen hoe substantiëler (symbolischer) de omgang met de GDPR.

In dit onderzoek zijn twee theorieën geïntegreerd. Enerzijds Stakeholder Theory en anderzijds Legitimacy Theory. Stakeholder Theory gaat er van uit dat organisaties voor hun existentie legitimiteit proberen te verkrijgen van afzonderlijke stakeholders. Legitimacy Theory gaat er van uit dat organisaties voor hun existentie legitimiteit trachten te verkrijgen van de maatschappij als geheel. Hierbij passen organisaties een mix toe van symbolische en substantiële legitimatie acties. Symbolische legitimatie acties zijn gericht op de beeldvorming extern en op het effectueren van (oppervlakkige) veranderingen aan de buitenkant van de organisatie op de korte termijn. Hiermee zegt de organisatie wat het doet. Substantiële legitimatie acties zijn gericht op de bedrijfsvoering intern en op het implementeren van (diepgaande) veranderingen aan de binnenkant van de organisatie op de lange termijn. Hiermee doet de organisatie wat het zegt. Het substantieel doorvoeren van legitimatie acties legt meer beslag op de middelen van een organisatie. Daarom neigen managers op korte termijn meer naar het symbolisch dan het substantieel doorvoeren van legitimatie acties. Als er echter te grote verschillen ontstaan tussen wat de organisatie zegt en wat de organisatie doet, neemt de organisatie op lange termijn het risico extra legitimatiekosten te moeten maken. Het substantieel implementeren van de GDPR zal ook meer beslag leggen op de middelen van een organisatie, zeker voor data intensieve organisaties, die veel persoonsgegevens verzamelen en verwerken. Organisaties die meer symbolisch omgaan met gegevensbeveiliging zullen op korte termijn minder legitimatie kosten maken, maar nemen op lange termijn een groter risico op schending van gegevens en daardoor op het maken van meer legitimatie kosten. Als er voldoende middelen beschikbaar zijn of als de verwachten baten hoger zijn dan de verwachte kosten van het verkrijgen of behouden van legitimiteit zullen managers daarom toch neigen naar meer substantiële legitimatie acties.

Uit de resultaten van dit onderzoek blijkt dat de mate van absolute Stakeholder Salience een significant verklarend effect heeft op symbolische versus substantiële legitimatie acties. Hoe lager de prioriteit die door stakeholders wordt toegekend aan Data Protection (in de perceptie van de organisatie), hoe meer symbolisch de legitimatieacties van de organisatie zijn i.r.t. de GDPR. Hoe hoger de prioriteit die door stakeholders wordt toegekend aan Data Protection (in de perceptie van de organisatie), hoe meer substantieel de legitimatieacties van de organisatie zijn i.r.t. de GDPR. Uit de resultaten van dit onderzoek blijkt ook dat de mate van relatieve Stakeholder Salience een significant verklarend effect heeft op symbolische versus substantiële legitimatie acties. Dit effect verschilt echter niet wezenlijk t.o.v. het effect van absolute Stakeholder Salience. Uit de resultaten van dit onderzoekt blijkt verder dat het bedrijfsresultaat een significant modererend effect heeft op de relatie tussen de saillantie van Data Protection en de omgang met de GDPR. Hoe meer middelen een organisatie beschikbaar heeft, hoe sterker het effect van de saillantie van Data Protection op de meer substantiële omgang met de GDPR. Hoe minder middelen een organisatie beschikbaar heeft, hoe sterker het effect op de meer symbolische omgang met de GDPR.

Een opvallende uitkomst in dit onderzoek is dat 95% van de ondernemingen een Data Protection Officer (DPO) heeft benoemd, terwijl deze benoeming waarschijnlijk niet voor alle in dit onderzoek bestudeerde ondernemingen verplicht is. Ook is het opvallend dat 89% van de ondernemingen de bescherming van gegevens heeft opgenomen in een gedragscode, maar dat slechts 37% van de ondernemingen werkt met een certificaat, die deze bescherming bekrachtigt. Bovendien is het opvallend dat 80% van de ondernemingen beschrijft audits uit te voeren, die de bescherming van persoonsgegevens toetsen en dat eveneens 80% van de ondernemingen beschrijft procedures te hebben, die de bescherming van persoonsgegevens ondersteunen, maar dat slechts 26% van de ondernemingen beschrijft een register te hebben, waarin de transactie van persoonsgegevens wordt gedocumenteerd. Eveneens is het opvallend dat 79% van de ondernemingen een privacy statement/policy heeft, dat compliant is met de GDPR en waarin ook de omgang met de privacy rechten van mensen is opgenomen, maar dat slechts 25% respectievelijk 15% van de ondernemingen beschrijft procedures/protocollen en IT-systemen te gebruiken voor het ondersteunen van deze privacy rechten van mensen. Hierbij is het ook opvallend dat slechts 24% respectievelijk 6% van de organisaties werkt volgens de principes van 'privacy by design' en 'privacy by default'. Hoewel dit verder niet onderzocht is, lijken de veel voorkomende maatregelen het minst ingrijpend te zijn. Deze lijken daarmee een meer symbolisch karakter te hebben. De maatregelen die betrekkelijk weinig voorkomen, lijken het meest ingrijpend te zijn. Deze lijken daarmee een meer substantieel karakter te hebben. Voor ondernemingen, die op grote schaal of bijzondere persoonsgegevens verzamelen/ verwerken, verdient het aanbeveling kritisch te kijken of en hoe maatregelen zijn genomen t.a.v. de realisatie van het transactieregister van persoonsgegevens, de technische en organisatorische opvolging van de privacy rechten van mensen en de adoptie van 'privacy by design & default'.

Dit onderzoek is gestart vanuit de onderbouwing dat symbolische en substantiële legitimatie acties min of meer elkaars tegenovergestelden zijn. Ook in veel andere onderzoeken werden deze behandeld als 'of/of' fenomenen. N.a.v. de hiervoor genoemde opvallende uitkomsten roept dit onderzoek echter de vraag op of symbolische en substantiële legitimatie acties niet beter als 'en/en' fenomenen te beschouwen zijn. Hierbij wordt het verschil van de legitimatie acties niet zo zeer bepaald door het karakter, zijnde oppervlakkig versus diepgaand, als wel door het doel, zijnde het beïnvloeden van de beeldvorming extern en/of het veranderen van de bedrijfsvoering intern. De mix en intensiteit van deze acties, lijkt afhankelijk te zijn van het effect dat organisaties er mee willen bereiken en van de saillantie van stakeholders. Dit onderzoek geeft hiervoor de volgende aanwijzingen:

- Voor het verkrijgen van legitimiteit lijkt voornamelijk de beeldvorming extern beïnvloed te moeten worden.
- Voor het behouden van legitimiteit lijkt de beeldvorming extern beïnvloed te moeten én lijkt de bedrijfsvoering intern (en daarmee ook de beeldvorming intern) veranderd te moeten worden.
- Naarmate de saillantie van stakeholders en de saillantie van de claims die stakeholders op de organisaties leggen toeneemt, lijkt de intensiteit van deze legitimatie acties toe te moeten nemen.
- Naarmate deze saillantie afneemt, lijkt de intensiteit van deze legitimatie acties af te kunnen nemen.

Naar deze afhankelijkheden en variaties in mix en intensiteit is verder onderzoek nodig.

In de wetenschap is nog steeds veel discussie over de perceptie van (managers van) organisaties op de saillantie van hun stakeholders en de mate waarin en wijze waarop dit resulteert in acties waarmee organisaties legitimiteit trachten te verkrijgen of te behouden. Dit onderzoek draagt bij aan deze discussie en geeft suggesties voor vervolgonderzoek. Dit onderzoek is ook relevant voor mensen, die onderzoek doen naar de CSR van organisaties en de ontsluiting van CSR informatie door organisaties. Daarnaast is dit onderzoek praktisch relevant voor bestuurders en managers, die betrokken zijn bij de ontwikkeling, uitvoering en handhaving van beleid m.b.t. Data Protection en de verantwoording hiervan aan hun stakeholders. Tenslotte is het onderzoek ook maatschappelijk relevant, omdat het een beeld geeft van de status van de omgang met de GDPR door beursgenoteerde organisaties.

Summary

In this research the dealing of organizations with the General Data Protection Regulation (GDPR) has been studied. Since the GDPR does not provide clear guidelines for this, organizations must decide for themselves how they implement the GDPR and how they comply with the GDPR. In this research the effect of the degree of Stakeholder Salience regarding Data Protection on a more symbolic or more substantive approach to the GDPR has been studied. Stakeholder Salience was determined by the extent to which stakeholders - in the perception of the managers of an organization - give priority to Data Protection. For this purpose a content analysis has been executed and annual reports and any Corporate Social Responsibility (CSR) reports, privacy statements and codes of conduct published in 2018 of 107 European companies listed on the main stock exchanges of Amsterdam, Brussels, Paris, Frankfurt, Dublin and Milan were examined. Stakeholder Salience was derived from the data out of the materiality matrices that these companies have published as part of the Global Reporting Initiative (GRI) guidelines as applied by these companies. The higher (lower) the score in the matrix, the higher (lower) the salience. Stakeholder Salience was measured in this study not only in an absolute sense (as a single priority), but also in a relative sense (as a weighted priority among multiple priorities). After all, managers have to deal with multiple stakeholders and multiple claims they make to the organization. Dealing with the GDPR was derived from the number of GDPR related measures that an organization has described in its public publications. Hereby 24 different measures were examined, which relate to different GDPR articles. The more (less) GDPR related measures, the more substantial (symbolic) the dealing with the GDPR.

In this research two theories were integrated. On the one hand Stakeholder Theory and on the other hand Legitimacy Theory. Stakeholder Theory implies that organizations try to obtain legitimacy for their existence from separate stakeholders. Legitimacy Theory implies that organizations try to obtain legitimacy from society as a whole for their existence. Hereto organizations apply a mix of symbolic and substantive legitimation actions. Symbolic legitimization actions are aimed at external imaging and at effecting (superficial) changes on the outside of the organization in the short term. With these an organization says what it does. Substantive legitimation actions are aimed at internal business operations and at implementing (profound) changes on the inside of the organization in the long term. With these the organization does what it says. Substantive legitimation actions do place greater demands on the resources of an organization than symbolic legitimation actions do. That is why managers in the short term tend to pursue more symbolic than substantive legitimation actions. However, if there are too great differences between what the organization says and what the organization does, the organization takes the long-term risk of incurring additional legitimation costs. Substantive implementation of the GDPR will also place greater demands on the resources of an organization, especially for data-intensive organizations that collect and process a lot of personal data. Organizations that more symbolically take care about data security will incur less legitimation costs in the short term, but in the long term will take a greater risk regarding data breaches and therefore will incur more legitimation costs. Therefore, if sufficient resources are available or if the expected benefits outweigh the expected costs of gaining or maintaining legitimacy, managers will tend tend to pursue more substantive legitimation actions.

The results of this research show that the degree of absolute Stakeholder Salience has a significant explanatory effect on symbolic versus substantive legitimation actions. The lower the priority given by stakeholders to Data Protection (in the perception of the organization), the more symbolic the legitimation actions of the organization are regarding the GDPR. The higher the priority given by stakeholders to Data Protection (in the perception of the organization), the more substantive the legitimation actions of the organization are regarding the GDPR. The results of this research also show that the degree of relative Stakeholder Salience has a significant explanatory effect on symbolic versus substantive legitimation actions. However, this effect does not differ significantly from the effect of absolute Stakeholder Salience. The results of this study further show that the 'operating income' has a significant moderating effect on the relationship between the salience of Data Protection and the dealing with the GDPR. The more resources an organization has available, the stronger the effect of the salience of Data Protection on the more substantive dealing with the GDPR. The fewer resources an organization has available, the stronger the effect on the more symbolic handling with the GDPR.

A remarkable result in this research is that 95% of the companies have appointed a Data Protection Officer (DPO), while this appointment is probably not mandatory for all companies examined in this research. It is also remarkable that 89% of the companies have included Data Protection within a code of conduct, but only 37% of the companies have a certificate that confirms this protection. In addition, it is noteworthy that 80% of the companies report that they carry out audits that assess the protection of personal data and that 80% of the

companies also report having procedures that support the protection of personal data, but that only 26% of the companies describe having a register that documents the transaction of personal data. It is also noteworthy that 79% of the companies have a privacy statement/policy, which is compliant with the GDPR and which also includes the handling of people's privacy rights, but only 25% and 15% of the companies describe procedures/ protocols and IT systems to support these privacy rights. It is also notable that only 24% and 6% of the organizations work according to the principles of 'privacy by design' and 'privacy by default'. Although this has not been further examined, the more common measures seem to be the least drastic. These seem to have a more symbolic character. The more uncommon measures seem to be the most drastic. These seem to have a more substantive character. For companies that collect/process large-scale or special personal data, it is recommended to critically examine whether and how measures have been taken with regard to the realization of the transaction register of personal data, the technical and organizational follow-up of the privacy rights of people and the adoption of 'privacy by design & default'.

This research did start with the substantiation that symbolic and substantive legitimation actions are more or less opposites. In many other studies these were also treated as 'or/or' phenomena. In response to the aforementioned remarkable results, however, this research raises the question whether symbolic and substantive legitimation actions can better be regarded as 'and/and' phenomena. The difference of the identification actions is not so much determined by the character, being superficial versus profound, but by the goal, which is to influence the external business image and / or to change the internal business processes. The mix and intensity of these actions seem to depend on the effect that organizations want to achieve with these actions and on the salience of stakeholders. This research provides the following indications for this:

- In order to gain legitimacy, it appears that the external business image needs to be influenced.
- In order to maintain legitimacy, it seems that the external business image has to be influenced and the internal business processes (and therefore also the internal business image) need to be changed.
- As the salience of stakeholders and the salience of the claims that stakeholders put on organizations increases, the intensity of the legitimation actions need to be increased.
- As this salience decreases, the intensity of these legitimation actions can be decreased.

Further research is needed into these dependencies and variations in mix and intensity.

There is still much debate within science about the perception of (managers of) organizations about the salience of their stakeholders and the extent to which and how this results in actions by which organizations try to gain or maintain legitimacy. This research contributes to this debate and provides suggestions for further research. This research is also relevant for people who study the CSR of organizations and the disclosure of CSR information by organizations. In addition, this research is practically relevant for executives and managers, who are involved in the development, implementation and enforcement of Data Protection policies and their accountable to their stakeholders. Finally, the research is also socially relevant, because it provides an overview of the status of the dealing with the GDPR by listed organizations.

Inhoudsopgave

1. Introductie

1.1. Achtergrond Onderzoek

In dit onderzoek wordt de omgang van organisaties met de General Data Protection Regulation (GDPR) of de Algemene Verordening Gegevensbescherming (AVG) bestudeerd. Deze verordening is sinds 25 mei 2018 van kracht. Hierdoor moeten persoonsgegevens beter beveiligd worden en moet de privacy van burgers beter beschermd worden. De GDPR geeft geen duidelijke richtlijnen voor de implementatie binnen organisaties, waardoor organisaties zelf moeten besluiten hoe zij de GDPR implementeren en hoe zij voldoen aan de GDPR (Tikkinen-Piri, Rohunen, & Markkula, 2018).

De omgang met de GDPR maakt deel uit van het IT-beleid van een organisatie. Bij het ontwikkelen en realiseren van dit beleid moet een organisatie rekening houden met haar stakeholders (Angst, Block, D'Arcy, & Kelley, 2017; Harguem, Karuranga, & Mellouli, 2014). Hierbij geeft een organisatie verschillende prioriteiten aan de claims, die deze stakeholders op de organisatie leggen. Deze prioritering is benoemd als Stakeholder Salience (Mitchell, Agle, & Wood, 1997). Dit concept is afgeleid van de Stakeholder Theory. Stakeholder Theory gaat er van uit dat organisaties voor hun existentie legitimiteit proberen te verkrijgen van afzonderlijke stakeholders (Chen & Roberts, 2010).

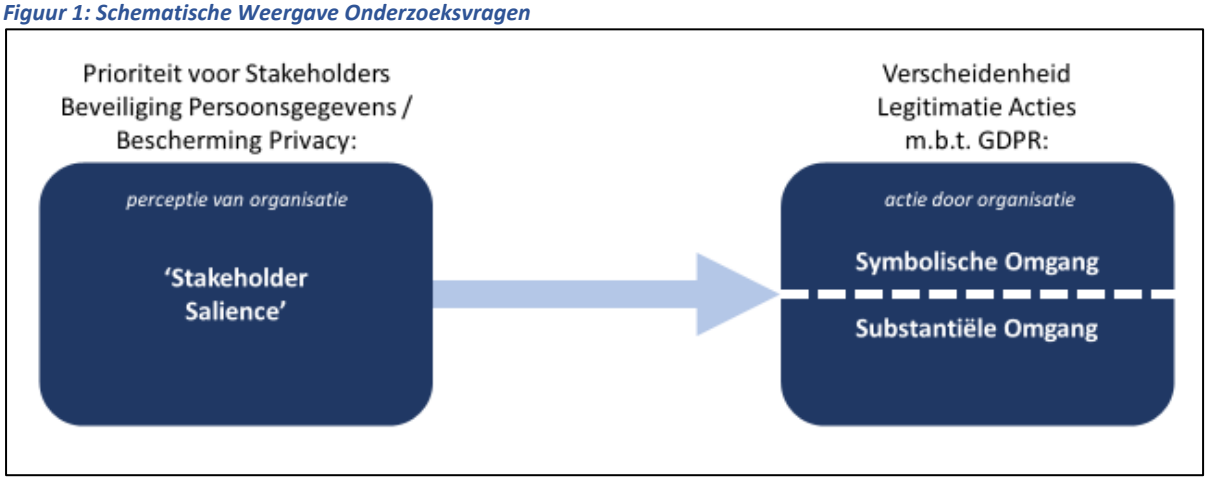
De omgang door organisaties met de GDPR is bestudeerd vanuit de Legitimacy Theory. Legitimacy Theory gaat er van uit dat organisaties voor hun existentie legitimiteit trachten te verkrijgen van de maatschappij als geheel (Chen & Roberts, 2010). Hierbij voeren organisaties een verscheidenheid uit aan symbolische (oppervlakkige) en substantiële (diepgaande) legitimatie acties (Ashforth & Gibbs, 1990). Hoe belangrijker stakeholders in gezamenlijkheid een onderwerp vinden en hoe meer dit onderwerp aansluit op de agenda van de organisatie, hoe substantiëler de response van de organisatie zal zijn (Ashforth & Gibbs, 1990).

In dit onderzoek wordt bestudeerd wat het effect is van de prioriteit die stakeholders aan Data Protection toekennen op een meer symbolische c.q. meer substantiële omgang met de GDPR. Concreet richt dit onderzoek zich op de hoofdvraag: **Wat is de invloed van de mate van Stakeholder Salience i.r.t. de beveiliging van persoonsgegevens en de bescherming van privacy op de mate van symbolische c.q. substantiële omgang met de GDPR door organisaties?** Om de hoofdvraag te kunnen beantwoorden worden eerst de onderstaande deelvragen beantwoord.

1. Welke mate van prioriteit geven stakeholders - in de perceptie van organisaties - aan de beveiliging van persoonsgegevens en de bescherming van de privacy van burgers?
2. Welke mate van verscheidenheid tussen symbolische en substantiële legitimatie acties voeren organisaties uit bij hun omgang met de GDPR?

Deze hoofd- en deelvragen zijn schematisch weergegeven in figuur 1.

Figuur 1: Schematische Weergave Onderzoeksvragen



1.2. Aanpak Onderzoek

Om de onderzoeksvragen te kunnen beantwoorden is eerst de literatuur systematisch onderzocht. Hieruit zijn hypothesen onttrokken. Vervolgens zijn data verzameld en geanalyseerd van Europese beursgenoteerde ondernemingen. Dit is gedaan m.b.v. een content analyse van de door deze ondernemingen gepubliceerde jaarverslagen, Corporate Social Responsibility (CSR) rapportages, privacy statements/policies en codes of

conduct/ethics. Bij de dataverzameling en -analyse zijn alleen beursgenoteerde ondernemingen meegenomen, die jaarverslagen en eventuele CSR rapportages hebben gepubliceerd volgens de richtlijnen van de Global Reporting Initiative (GRI) én die een Materiality Matrix hebben opgesteld, waarin de materiële punten voor de organisatie en haar stakeholders zijn benoemd.

1.3. Relevantie Onderzoek

Er is nog steeds veel discussie in de wetenschap over de perceptie van organisaties op de saillantie van hun stakeholders en de mate waarin en wijze waarop dit resulteert in acties waarmee organisaties legitimiteit trachten te verkrijgen (Bundy, Shropshire, & Buchholtz, 2013; Durand, Hawn, & Ioannou, 2019; Kuruppu, Milne, & Tilt, 2019). Dit onderzoek draagt bij aan deze discussies door het effect te bestuderen van Stakeholder Salience op symbolische versus substantiële legitimatie acties. Naar dit effect is nog relatief weinig onderzoek verricht. Hiermee ontstaat wetenschappelijke relevantie van dit onderzoek. Met de kennis, die hiermee vergaard wordt kan beter begrepen worden hoe stakeholders en managers van organisaties over en weer hun invloeden en interventies beter op elkaar kunnen afstemmen (Cundill, Smart, & Wilson, 2018). Hiermee ontstaat ook praktische relevantie van dit onderzoek.

Naar de invloed van Stakeholder Salience op de symbolische versus substantiële omgang met de GDPR of andere verordeningen gericht op beveiliging van persoonsgegevens en bescherming van privacy is, voor zover bekend, nog helemaal geen onderzoek verricht. Hiermee draagt dit onderzoek ook bij aan de ontwikkeling van kennis over de CSR van organisaties en het ontsluiten van CSR informatie door organisaties i.r.t. de beveiliging van persoonsgegevens en de bescherming van privacy. Hiermee is het onderzoek wetenschappelijk relevant, voor mensen die in algemeenheid onderzoek doen naar CSR en CSR ontsluiting. Daarnaast is dit onderzoek praktisch relevant voor bestuurders en managers, die betrokken zijn bij de ontwikkeling, uitvoering en handhaving van beleid m.b.t. Data Protection en de verantwoording hiervan aan hun stakeholders. Tenslotte is het onderzoek ook maatschappelijk relevant, omdat het een beeld geeft van de status van de omgang met de GDPR door - in dit geval beursgenoteerde - organisaties.

2. Theoretisch kader

2.1. Aanpak Literatuurstudie

Om de onderzoeksvragen te kunnen beantwoorden is eerst de literatuur systematisch onderzocht. In eerste instantie is naar bronnen gezocht m.b.v. de databases van Ebsco Host en Google Scholar. Hierbij is gezocht op de onderwerpen: General Data Protection Regulation (GDPR), Stakeholder Theory/Management, Stakeholder Salience, Legitimacy Theory, Symbolic/Substantive Legitimacy, CSR Disclosure en Global Reporting Initiative (GRI). Hierbij zijn ook verdiepingen gezocht naar IT-Management en Data Protection/Security. In tweede instantie is hierbij naar bronnen gezocht die verwijzen naar wat 2 cruciale artikelen blijken te zijn. De één heeft betrekking op Stakeholder Salience, zijnde van Mitchell et al. (1997). De ander heeft betrekking op Symbolic/Substantive Legitimacy, zijnde van Ashforth & Gibbs (1990). Van de gevonden bronnen zijn er, na beoordeling van 'title' en 'abstract', 79 als relevant beoordeeld. Na bestudering van met name de inleiding en conclusies van deze 79 bronnen zijn in totaal 28 bronnen geselecteerd, die zijn gebruikt bij de beantwoording van de onderzoeksvragen. Een gedetailleerd overzicht van deze systematische literatuurstudie, inclusief zoeksleutels/-filters is opgenomen in bijlage 1a. Een overzicht van de gevonden relevante bronnen en uiteindelijk geselecteerde bronnen is opgenomen in bijlage 1b.

2.2. Bevindingen Literatuurstudie

General Data Protection Regulation (GDPR)

De General Data Protection Regulation (GDPR) is goedgekeurd door het Europees Parlement op 14 april 2016 en is op 25 mei 2018 in werking getreden. Deze verordening heeft vanaf dat moment de Data Protection Directive vervangen, die sinds 13 december 1995 in de Europese Unie van kracht was. De nieuwe verordening regelt de rechtmatige en zorgvuldige omgang met persoonsgegevens binnen de Europese Unie. Met deze verordening zijn twee belangen gemoeid: de bescherming van persoonsgegevens én de bevordering van de vrije uitwisseling van persoonsgegevens (Schermer, Hagenauw, & Falot, 2018). De verordening is van toepassing op iedere verwerking van persoonsgegevens (Engelfriet, Chew-Meij, & Kager, 2018) en geldt voor organisaties die voor de verwerking verantwoordelijk zijn (de 'data controller') en voor organisaties die de verwerking verzorgen (de 'data processor'). Persoonsgegevens zijn gegevens over een geïdentificeerde of identificeerbare natuurlijke persoon. Gepseudonimiseerde gegevens zijn wel nog te herleiden naar een natuurlijke persoon. Geanonimiseerde gegevens niet meer. De verordening is daarom wel van toepassing op gepseudonimiseerde gegevens, maar niet op geanonimiseerde gegevens (Engelfriet et al., 2018; Schermer et al., 2018). De implementatie van de GDPR grijpt in op de operatie van organisaties en vormt daarom voor veel organisaties, zeker voor data intensieve organisaties, een grote uitdaging, die een wezenlijk beslag legt op hun middelen (Tikkinen-Piri et al., 2018).

De GDPR bevat zelf geen instructies voor de implementatie (Tikkinen-Piri et al., 2018). Om GDPR compliant te worden moeten organisaties zelf hun processen en procedures opnieuw beoordelen en inrichten (Teixeira, da Silva, & Pereira, 2019). In verschillende onderzoeksrapporten in de aanloop naar 25 mei 2018 werd aangegeven dat slechts 34% tot 51%[1] van de organisaties tijdig GDPR compliant zou zijn. Organisaties die niet GDPR compliant zijn, kunnen hiervoor boetes krijgen, die kunnen oplopen tot 4% van hun wereldwijde omzet (artikel 83 GDPR). Ieder EU-land heeft een nationale autoriteit toegewezen die toeziet op de naleving van de GDPR. In de GDPR staan verplichte maatregelen genoemd, waarmee organisaties aan hun verantwoordingsplicht voldoen. Dit zijn:

- bijhouden van gegevensverwerkingsregister;
- aantonen van passend gegevensbeschermingsbeleid;
- onderbouwen van al dan niet aanstellen van een Data Protection Officer (DPO) of Functionaris Gegevensbescherming (FG)
- uitvoeren van Data Protection Impact Assessment (DPIA) voor gegevensverwerkingen met een hoog privacy risico;
- bijhouden van register van opgetreden datalekken (ook als deze niet gemeld hoeven te worden);
- aantonen dat een betrokkene daadwerkelijk toestemming heeft gegeven voor de verwerking van zijn/haar persoonsgegevens;
- documenteren van processen en procedures ter waarborging van de privacy rechten van de betrokkenen;

[1] Door *iWelcome* in 'The state of GDPR-readiness in Europe': 34%. Door *Senzing* in 'Finding the missing link in GDPR compliance': 40%. Door *PWC* in 'Privacy Governance Onderzoek': 42%. Door *Capgemini* in 'Seizing the GDPR advantage': 51%.

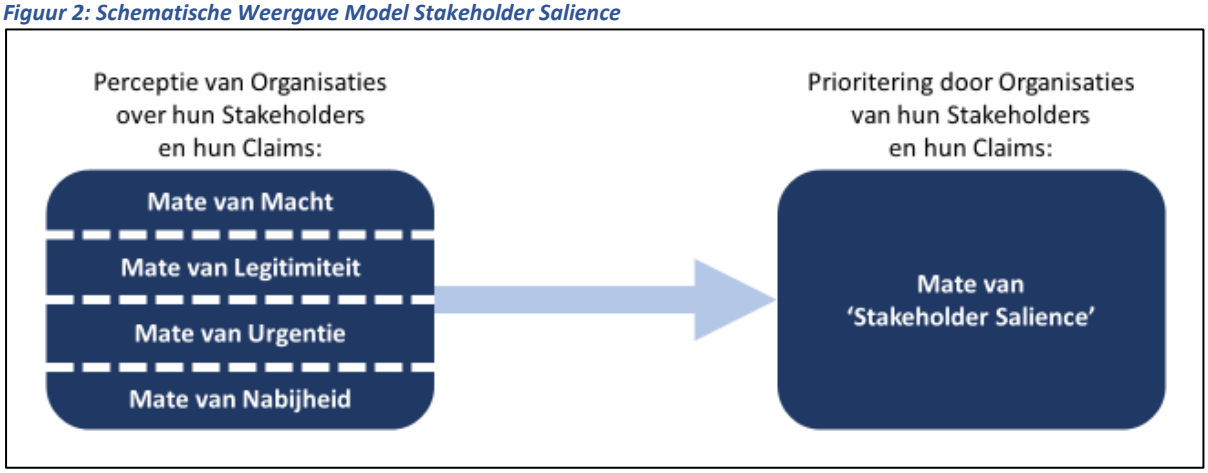
- schriftelijk informeren van betrokkenen in een verklaring (bijvoorbeeld in de vorm van een privacy statement) over hun privacy rechten;

Naast de verplichte maatregelen kunnen organisaties ook vrijwillig extra maatregelen nemen, zoals het behalen van certificaten, het aansluiten bij gedragscodes en het afleggen van verantwoording in jaarverslagen over het beleid m.b.t. de verwerking en beveiliging van persoonsgegevens.

Stakeholder Salience

Binnen en buiten een organisatie zijn verschillende groepen belanghebbenden of stakeholders te onderkennen. Deze stakeholders proberen invloed uit te oefenen op het beleid van de organisatie en omgekeerd proberen organisaties met hun beleid invloed uit te oefenen op hun stakeholders (Freeman, 1984). Organisaties proberen met en voor deze belanghebbenden waarde te creëren en proberen hierbij rekening te houden met hun belangen (Freeman, 1984; Griffin, 2017; Myllykangas, Kujala, & Lehtimäki, 2011). Stakeholders kunnen onderling verschillende belangen hebben, die concurrerend kunnen zijn met, maar ook complementair kunnen zijn aan elkaars belangen (Chen & Roberts, 2010; Griffin, 2017). Deze verschillende belangen kunnen conflicterend zijn met, maar ook consistent zijn aan de logica van de organisatie (Bundy et al., 2013). Organisaties geven aan belanghebbenden en hun belangen verschillende prioriteiten. De mate waarin managers hieraan prioriteit geven is in de literatuur benoemd als Stakeholder Salience. Dit is door Mitchell et al. (1997) gedefinieerd als '*the degree to which managers give priority to competing stakeholderclaims*'. Zij onderscheiden hierbij het 'wie' (de stakeholders) en het 'wat' (hun claims). De kern van deze theorie is dat managers meer prioriteit aan stakeholders zullen geven als deze stakeholders als meer saillant worden ervaren. Dit is afhankelijk van de mate van macht, legitimiteit, urgentie die aan stakeholders wordt toegekend (Mitchell et al., 1997). Naarmate meer van deze verschillende attributen worden toegekend aan een belanghebbende, zal deze belanghebbende als meer saillant ervaren worden en dus meer prioriteit gegeven worden. De theorie en het construct met de bijbehorende attributen is oorspronkelijk ontwikkeld door Mitchell et al. (1997). Door o.a. Neville, Bell, & Whitwell (2011) en Khurram & Petit (2017) zijn herzieningen voorgesteld. De verschillen tussen het oorspronkelijke model en de voorstellen voor herziening zijn uitgebreid uitgewerkt in bijlage 2. Door Neville et al. (2011) wordt betoogd dat de verschillende attributen in meerdere of mindere mate aanwezig kunnen zijn. Door Khurram & Petit (2017) is het attribuut nabijheid toegevoegd. Dit past beter bij de tegenwoordige tijd, waarin posities in (virtuele en reële) netwerken steeds belangrijker zijn geworden. Het (herziene) model Stakeholder Salience is schematisch uitgewerkt in figuur 2.

Figuur 2: Schematische Weergave Model Stakeholder Salience



Het model van Stakeholder Salience maakt het voor managers mogelijk afzonderlijke stakeholders te identificeren en prioriteren. Dit model is ook toepasbaar in de context van IT (Harguem et al., 2014). Het identificeren en prioriteren van stakeholders is een dynamisch proces. Bij de bestudering van de literatuur zijn verschillende afhankelijkheden gevonden, die deze dynamiek beïnvloeden. Ten eerste kunnen managers de saillantie van een belanghebbende (Jawahar & McLaughlin, 2001; Khurram & Petit, 2017; Mitchell et al., 1997) en zijn belang (Bundy et al., 2013) na verloop van tijd anders beoordelen. Ten tweede houden managers niet met één stakeholder afzonderlijk, maar met verschillende stakeholders tegelijkertijd rekening (Griffin, 2017; Kuruppu et al., 2019; Mitchell, Lee, & Agle, 2017; Neville et al., 2011). Dit punt leidt tot hypothese 2 (zie paragraaf 2.3). Ten derde houden managers niet alleen rekening met het belang dat een onderwerp heeft voor stakeholders, maar ook met de significantie van dit onderwerp voor de missie en de strategie van de organisatie (Ashforth & Gibbs, 1990; Bundy et al., 2013; Bundy, Vogel, & Zachary, 2018; Myllykangas et al., 2011). Hoewel Stakeholder Salience veel aandacht en aanprijzing heeft gehad in verschillende studies, is er ook nog veel

discussie over dit model, waardoor verdere verbetering en verfijning en meer onderzoek naar de inhoud en context nodig zijn (Joos, 2019; Khurram, Pestre, & Petit, 2019; Mitchell et al., 2017).

'substantive versus symbolic' legitimatie

Een organisatie verkrijgt haar legitimiteit door zich te conformeren aan maatschappelijke normen, waarden en verwachtingen (Ashforth & Gibbs, 1990). Deze status verkrijgt de organisatie in wisselwerking met haar stakeholders (Angst et al., 2017; Ashforth & Gibbs, 1990; Chen & Roberts, 2010). Bij het vergroten, handhaven, of verdedigen van deze status passen organisaties een mix van 'substantive' en 'symbolic' legitimatie acties toe, die na verloop van tijd kan veranderen (Ashforth & Gibbs, 1990). Ook in het domein van IT en gegevensbeveiliging maken organisaties een keuze tussen een meer substantiële of een meer symbolische benadering (Angst et al., 2017). Bij de bestudering van de literatuur zijn verschillende kenmerken gevonden, waarmee auteurs substantiële en symbolische legitimatie acties beschrijven. Deze kenmerken zijn benoemd in figuur 3.

Figuur 3: Kenmerken Substantiële en Symbolische Legitimatie Acties

Auteurs	Substantiële Legitimatie Acties	Symbolische Legitimatie Acties
Angst et al. (2017)	zijn vastgekoppeld aan de dagelijkse activiteiten van de organisatie en zijn gericht op de lange termijn	zijn losgekoppeld van de dagelijkse activiteiten van de organisatie en zijn gericht op de korte termijn
Ashforth & Gibbs (1990)	leiden tot daadwerkelijke, diepgaande verandering van de doelstellingen, structuren, processen en praktijken van de organisatie	leiden tot ogenschijnlijke, oppervlakkige verandering van de organisatie
Perez-Batres, Doh, Miller, & Pisani (2012)	gaan (min of meer vrijwillig) verder dan wettelijke bepalingen	komen minimaal tegemoet aan wettelijke bepalingen
Durand et al. (2019)	hebben een strikte, formele benadering en gaan gepaard met het nakomen van beloften	hebben een losse, informele benadering en gaan gepaard met het doen van beloften
Ashforth & Gibbs (1990); Durand et al. (2019); Perez-Batres et al. (2012); Schons & Steinmeier (2016)	kosten meer moeite om te realiseren en doen een groter beroep op de middelen van de organisatie	kosten minder moeite om te realiseren en doen een kleiner beroep op de middelen van de organisatie
Hyatt & Berente (2017)	zijn proactief en gericht op het beïnvloeden van interne belanghebbenden	zijn reactief en gericht op het beïnvloeden van externe belanghebbenden
Shabana & Ravlin (2016)	vormen stakeholders met kennis over de organisatie	misleiden stakeholders met informatie over de organisatie

Uitgaande van voorgaande beschrijvingen, hebben substantiële legitimatieacties als gemeenschappelijk kenmerk dat deze intrinsiek gedreven zijn en gericht zijn op de bedrijfsvoering intern en de lange termijn. Kortom: hiermee doet de organisatie wat het zegt. Uitgaande van voorgaande beschrijvingen, hebben symbolische legitimatie acties als gemeenschappelijk kenmerk dat zij extrinsiek gedreven zijn en gericht zijn op de beeldvorming extern en de korte termijn. Kortom: hiermee zegt de organisatie wat het doet.

Omdat het substantieel doorvoeren van legitimatie acties meer beslag legt op de middelen van een organisatie, zullen de managers van een organisatie in beginsel meer neigen naar het symbolisch dan het substantieel doorvoeren van legitimatie acties (Ashforth & Gibbs, 1990). Als er echter grote verschillen ontstaan tussen wat de organisatie zegt en wat de organisatie doet dan zal dit door stakeholders bekritiseerd worden (Schons & Steinmeier, 2016), waardoor de organisatie later het risico loopt extra legitimatie kosten te moeten maken. Organisaties die meer symbolisch omgaan met gegevensbeveiliging zullen op korte termijn minder kosten nodig hebben om hun legitimiteit op dit punt te verkrijgen, maar lopen op lange termijn een groter risico op schending van gegevens en zullen daardoor meer kosten nodig hebben om hun legitimiteit op dit punt te onderhouden c.q. te repareren. Als er voldoende beschikbare middelen zijn (Perez-Batres et al., 2012) of als de verwachte baten hoger zijn dan de verwachte kosten (Durand et al., 2019) zullen managers toch neigen naar meer substantiële legitimatie acties. Deze beschouwingen hebben geleid tot hypothese 3 (zie paragraaf 2.3).

effect van Stakeholder Salience op symbolische / substantiële legitimatie acties

Door het nemen van legitimatie acties proberen organisaties legitimiteit te verkrijgen van afzonderlijke groepen stakeholders en van de maatschappij als geheel (Chen & Roberts, 2010). Hierbij wordt gestreefd naar congruentie tussen de waarden systemen van de organisatie, de waarden systemen van groepen stakeholders en de waarden systemen van de maatschappij (Chen & Roberts, 2010). Hoewel hierbij aannemelijk is dat organisaties, bij hun keuze voor symbolische / substantiële legitimatie acties, rekening houden met de mate van

saillantie van stakeholders, is dit verband nog amper onderzocht en aangetoond. Bij de bestudering van de literatuur is slechts een klein aantal onderzoekers gevonden, die dit verband enigszins heeft bestudeerd of hiervoor een voorzet heeft gegeven. De door hen onderzochte dan wel verwachte effecten zijn benoemd in figuur 4. Deze leiden tot hypothese 1 (zie paragraaf 2.3).

Figuur 4: Effecten Stakeholder Salience op Substantiële en Symbolische Legitimatie Acties

Auteurs / Onderzoeksmethode	Effect Stakeholder Salience op Legitimatie Acties
Perez-Batres et al. (2012) / kwantitatief onderzoek; KLD (nu MSCI) dataset	Als stakeholders een organisatie een lage beoordeling geven, dan zal een organisatie in reactie symbolische legitimatie acties nemen, want het risico op imagoschade is dan laag. Als stakeholders een organisatie een hoge beoordeling geven, dan zal een organisatie in reactie substantiële legitimatie acties nemen, want het risico op imagoschade is dan hoog.
Perez-Batres et al. (2012) / kwantitatief onderzoek; KLD (nu MSCI) dataset	Naarmate een organisatie langere tijd meer reguleringsdruk ervaart van stakeholders (ongeacht of deze druk van buiten of binnen de sector opgevoerd wordt), zal een organisatie meer substantieel dan symbolisch op deze druk reageren.
Bundy et al. (2013) / conceptueel voorstel	Issues die gerelateerd zijn aan de identiteit (de waarden) én de strategie (de doelen) van de organisatie, leiden tot een hoge Issue Salience, die leidt tot substantiële legitimatie acties. Issues, die gerelateerd zijn aan de identiteit óf de strategie van de organisatie, leiden tot een middelmatige Issue Salience, die leidt tot symbolische legitimatie acties. Issues die niet gerelateerd zijn aan de identiteit of de strategie van de organisatie leiden tot een lage Issue Salience, die niet leidt tot legitimatie acties.
Durand et al. (2019) / conceptueel voorstel	Als de verwachte kosten van een legitimatie actie hoger zijn dan de baten, zal de organisatie eerder symbolisch reageren, zelfs als de issue hoog saillant is. Als de verwachte baten van een legitimatie actie hoger zijn dan de kosten, zal de organisatie eerder substantieel reageren, zelfs als de issue laag saillant is. Als de kosten veel groter zijn dan de baten kan het zelfs zo zijn dat een organisatie helemaal niet reageert.
Hyatt & Berente (2017) / kwalitatief onderzoek; survey	Een hoge druk van externe stakeholders leidt tot symbolische legitimatie acties om als organisatie een positief beeld op te roepen in de omgeving. Een hoge druk van interne stakeholders leidt tot substantiële legitimatie acties (gedreven door een geïnternaliseerd, vrijwillig commitment) om als organisatie een bepalende positie in de omgeving in te nemen.
Kuruppu et al. (2019) kwalitatief onderzoek; semi-gestructureerde interviews	Als een issue voor saillante stakeholders duidelijk waarneembaar is of (via minder saillante stakeholders) duidelijk waarneembaar wordt, zal een organisatie direct acties moeten nemen om legitimiteit op langere termijn te waarborgen. Als dit niet zo is kan een organisatie volstaan met het meer symbolisch rapporteren over deze issue.
Schons & Steinmeier (2016) / kwantitatief onderzoek; Thomson Reuters'Asset4SG Dataset	Stakeholders met een lage nabijheid tot de organisatie zijn ook te overtuigen met symbolische legitimatie acties. Stakeholders met een hoge nabijheid tot de organisatie zijn alleen te overtuigen met substantiële legitimatie acties.

CSR publicaties

In de dialoog met hun stakeholders en de samenleving als geheel geven organisaties informatie over de ontwikkeling en uitvoering van hun beleid. Deze informatie wordt deels verplicht en deels vrijwillig verstrekt. De kwaliteit van de publicaties, waarin deze vrijwillige informatie door organisaties wordt verstrekt, wordt betwist (Michelon, Pilonato, & Ricceri, 2015). Veel organisaties volgen een symbolische benadering bij het publiceren van hun jaarverslagen en hun eventuele CSR rapportages (Michelon et al., 2015). Uitzondering hierop zijn organisaties, die bij hun publicaties gebruik maken van de richtlijnen van het Global Reporting Initiative (GRI). De organisaties die deze richtlijnen gebruiken lijken een meer substantiële benadering te hebben (Michelon et al., 2015; Perez-Batres et al., 2012). De GRI richtlijnen vormen de standaard, die organisaties wereldwijd het meest gebruiken om over hun CSR beleid te rapporteren (del Mar Alonso-Almeida, Llach, & Marimon, 2014). Door deze richtlijnen te gebruiken geven organisaties standaard over meer onderwerpen informatie en is de informatie over deze onderwerpen tussen organisaties onderling beter vergelijkbaar (Marimon, Alonso-Almeida, Rodríguez, & Cortez Alejandro, 2012).

2.3. Conclusies Literatuurstudie en Hypothesen Onderzoek

Conclusies effect Stakeholder Salience op 'symbolic' versus 'substantive' legitimatie

Uit de literatuurstudie blijkt dat er naar Stakeholder Salience en symbolische versus substantiële legitimatie afzonderlijk relatief veel onderzoek is verricht. In de algemene context van de Corporate Social Responsibility

(CSR) van organisaties zijn deze onderwerpen uitgebreid onderzocht, maar in de specifieke context van gegevensbeveiliging en privacybescherming zijn deze onderwerpen niet of nauwelijks onderzocht. Uit de literatuurstudie blijkt ook dat er naar de samenhang tussen Stakeholder Salience en symbolische versus substantiële legitimatie relatief weinig onderzoek is verricht. De kwantitatieve onderzoeken van Perez-Batres et al. (2012) en Schons & Steinmeier (2016) en de kwalitatieve onderzoeken van Hyatt & Berente (2017) en Kuruppu et al. (2019) vormen hier een uitzondering op. Deze onderzoeken geven aanwijzingen dat een lage Stakeholder Salience leidt tot meer symbolische legitimatie acties en dat een hoge Stakeholder Salience leidt tot meer substantiële legitimatie acties. Het onderzoek van Perez-Batres et al. (2012) geeft een aanwijzing dat de hoeveelheid beschikbare middelen hierop een modererend effect heeft. Er is geen onderzoek gevonden dat de effecten van Stakeholder Salience i.r.t. gegevensbeveiliging en privacybescherming op een symbolische c.q. substantiële omgang met de GDPR beeft bestudeerd.

Conclusies definitie Stakeholder Salience

Uit de literatuurstudie blijkt dat er van Stakeholder Salience enigszins verschillende interpretaties zijn. Door Mitchell et al. (1997) is Stakeholder Salience oorspronkelijk gedefinieerd als '*the degree to which managers give priority to competing stakeholderclaims*'. Uit de eerder genoemde studies, waarin het verband is bestudeerd tussen Stakeholder Salience en symbolische versus substantiële legitimatie, zijn verschillende interpretaties van Stakeholder Salience af te leiden:

- de mate van positieve en negatieve percepties van stakeholders over een organisatie, mede gebaseerd op (CSR) 'rankings' en 'ratings' van deskundige derde partijen (Perez-Batres et al., 2012)
- de mate waarin aanspraken van stakeholders saillant zijn voor een organisatie, oftewel Issue Salience (Bundy et al., 2013; Durand et al., 2019)
- de mate van normatieve druk van interne en externe stakeholders gepercipieerd door de organisatie (Hyatt & Berente, 2017)
- de mate van onderlinge verbondenheid tussen (saillante en minder saillante) stakeholders (Kuruppu et al., 2019)
- de mate van nabijheid en betrokkenheid van stakeholders bij een organisatie (Schons & Steinmeier, 2016)

Hoewel de interpretaties van Stakeholder Salience in deze onderzoeken afwijken van de oorspronkelijke definitie, sluiten deze wel aan bij de theorie dat een verschil in saillantie leidt tot verschillende afwegingen en prioriteringen bij (de managers van) een organisatie.

In deze studie wordt de volgende definitie gehanteerd: Stakeholder Salience is de mate, waarin (managers van) organisaties prioriteit geven aan de aanspraken die stakeholders op de organisatie maken.

Conclusies definitie 'symbolic' versus 'substantive' legitimatie

In de eerder genoemde studies, waarin de relatie is bestudeerd tussen Stakeholder Salience en de acties, die de organisatie neemt om legitimiteit van hun stakeholders te verkrijgen of te behouden, wordt een mix onderkend van substantiële en symbolische legitimatie acties. Tegelijkertijd wordt er een duidelijk verschil onderkend tussen deze acties, waarbij er sprake lijkt van een continuüm, waarin een organisatie óf meer symbolische óf meer substantiële legitimatie acties neemt. In deze studie wordt er in beginsel van uit gegaan dat een organisatie een mix toepast, maar dat een combinatie van een hoge mate van symbolische legitimatie acties én een hoge mate van substantiële legitimatie acties elkaar zullen uitsluiten.

In deze studie worden de volgende definities gehanteerd: symbolische legitimatie acties zijn acties, die de organisatie neemt om legitimiteit te verkrijgen van hun stakeholders en die op korte termijn de beeldvorming over de organisatie beïnvloeden; substantiële legitimatie acties zijn acties, die de organisatie neemt om legitimiteit te verkrijgen van hun stakeholders en die op lange termijn de bedrijfsvoering van de organisatie beïnvloeden.

Hypothesen

Na bestudering van de literatuur zijn de volgende hypothesen opgesteld:

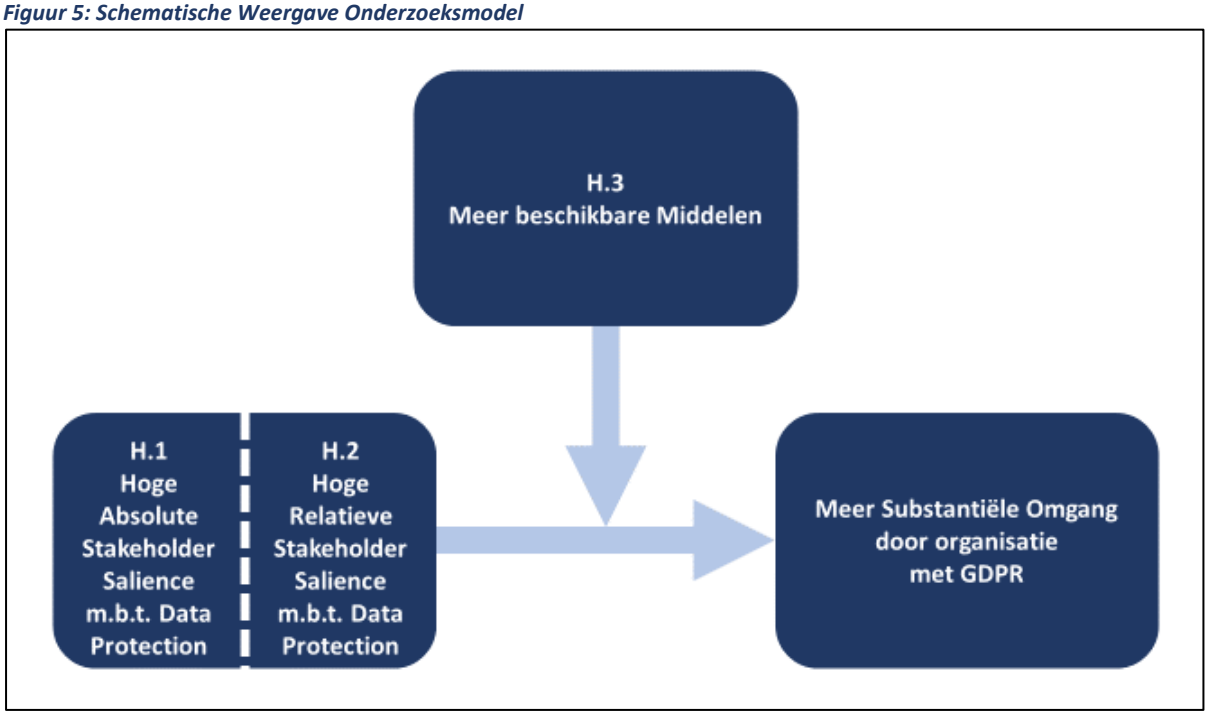
H.1 Als stakeholders (in de perceptie van managers van een organisatie) een hoge (lage) absolute prioriteit geven aan Data Protection zal een organisatie een meer substantiële (symbolische) omgang hebben met de GDPR.

H.2 Als stakeholders (in de perceptie van managers van een organisatie) een hoge (lage) relatieve prioriteit geven aan Data Protection t.o.v. andere onderwerpen zal een organisatie een meer substantiële (symbolische) omgang hebben met de GDPR.

H.3 Als een organisatie meer (minder) middelen ter beschikking heeft, dan zal dit een modererend effect hebben op een meer substantiële (symbolische) omgang met de GDPR.

Deze hypothesen zijn schematisch weergegeven in het onderzoeksmodel in figuur 5.

Figuur 5: Schematische Weergave Onderzoeksmodel



3. Methodologie

3.1. Conceptueel ontwerp: keuze van onderzoeksmethode

Data verzameling

Bij de data verzameling is gebruik gemaakt van de gegevens uit officiële jaarverslagen en eventuele separate CSR rapportages over 2018 (het jaar waarin de GDPR voor het eerst van kracht was) van in totaal 170[2] Europese ondernemingen, die genoteerd zijn aan de hoofdbeurzen van Amsterdam, Brussel, Parijs, Frankfurt, Dublin, en Milaan, zijnde respectievelijk AEX25, BEL20, CAC40, DAX30, ISEQ20, en MIB40. Hierbij is ook gebruik gemaakt van aanvullende gegevens uit privacy statements/policies en codes of conduct/ethics, voor zover deze op de website van deze ondernemingen stonden. Deze beursgenoteerde ondernemingen verrichten uiteenlopende kernactiviteiten, maar alle verzamelen en verwerken persoonsgegevens van hun medewerkers en van eventuele vertegenwoordigers van hun samenwerkingspartners. Sommige ondernemingen zullen daarbij nog persoonsgegevens verzamelen en verwerken van hun (potentiële) klanten. Dit betekent dat de GDPR voor al deze organisaties relevant is. De impact van de GDPR zal echter verschillend zijn, omdat de ene organisatie meer data intensief is dan de andere en de ene organisatie meer persoonsgegevens verwerkt dan de andere.

Binnen deze groep van 170 is een verdere selectie gemaakt van ondernemingen, die in hun publicaties gebruik maken van de richtlijnen van het Global Reporting Initiative (GRI) én die in hun publicaties een zogenaamde materialiteitsmatrix hebben opgenomen. Binnen de groep van 170 bleken 107 ondernemingen de GRI-richtlijnen toe te passen én een materialiteitsmatrix opgenomen te hebben in hun jaarverslag c.q. CSR-rapport. 63 ondernemingen hebben of geen GRI-richtlijnen toegepast of geen materialiteitsmatrix opgenomen. De data verzameling is daarom beperkt gebleven tot deze 107 ondernemingen. Dit is een methodologische keuze. Hiervoor zijn 3 verschillende redenen. Ten eerste, omdat de data in publicaties, die gebaseerd zijn op de GRI-standaard onderling beter vergelijkbaar zijn en daardoor geschikter om te analyseren dan de data uit publicaties, die niet op deze standaard gebaseerd zijn (Marimon et al., 2012). Ten tweede, omdat in deze standaard (i.t.t. de standaard van de United Nations[3], die ook door veel ondernemingen wordt toegepast), Customer Privacy één van de relevante onderwerpen is (GRI 200: Economic Standards 2016, GRI 300: Environmental Standards 2016 en GRI 400: Social Standards 2016), waarover een organisatie kan rapporteren. Deze GRI standaard adresseert '*the topic of customer privacy, including losses of customer data and breaches of customer privacy. These can result from non-compliance with existing laws, regulations and/or other voluntary standards regarding the protection of customer privacy*' (GRI 418: Customer Privacy 2016). De bedoeling van deze standaard sluit aan bij de bedoeling van de GDPR, namelijk het beveiligen van persoonsgegevens en het beschermen van de privacy van personen. Ten derde, omdat de materialiteitsmatrix (GRI 101: Foundation 2016), 2 dimensies bevat, waarvan er (in ieder geval) één voor dit onderzoek relevant is. De eerste dimensie is de mate van significantie van een onderwerp voor stakeholders. Deze dimensie sluit aan bij de definitie van Stakeholder Salience, zijnde de mate waarin (managers van) organisaties prioriteit geven aan de aanspraken die stakeholders op de organisatie maken. De tweede dimensie is de mate van significantie van een onderwerp voor de waarde creatie van de organisatie. Waar de eerste dimensie de saillantie van het onderwerp aangeeft voor stakeholders van de organisatie, geeft de tweede dimensie dus eigenlijk de saillantie aan van het onderwerp voor de managers van de organisatie.

Aangezien Stakeholder Salience en 'substantiële versus symbolische' legitimatie na verloop van tijd binnen een organisatie kan veranderen, zou het wetenschappelijk interessant zijn ook data uit eerdere jaren te verzamelen en te analyseren. De GDPR was toen nog niet van kracht, maar wel de voorganger van de GDPR, de Europese Privacyrichtlijn uit 1995. Hiermee zou onderzocht kunnen worden hoe de prioritering van de beveiliging van persoonsgegevens en de bescherming van de privacy van personen aan verandering onderhevig is geweest. Door de beperkte tijd is er echter voor gekozen dit niet te onderzoeken.

Data analyse

De data analyse is gedaan d.m.v. een content analyse. Dit is een techniek, waarbij kwalitatieve data gecodeerd, gecategoriseerd en numeriek gemaakt worden, zodat deze data kwantitatief geanalyseerd kunnen worden (Riffe, Lacy, Fico, & Watson, 2019; Saunders, Lewis, & Thornhill, 2016). Content analyse wordt veel toegepast bij studies naar de publicaties van organisaties i.r.t. CSR (Moratis & Brandt, 2017). Het voordeel hiervan is dat op

[2] In totaal zijn er 175 beursnoteringen, maar 5 hiervan komen dubbel voor.
[3] In de standaard van United Nations zijn 17 Sustainable Development doelstellingen benoemd, waarover een organisatie kan rapporteren. Binnen deze standaard is het beveiligen van persoonsgegevens en beschermen van de privacy echter niet als specifiek onderwerp beschreven.

een systematische manier vergelijkbare data verzameld en geanalyseerd kunnen worden van verschillende organisaties. Hiermee zijn de hypothesen te toetsen, zoals deze zijn afgeleid van de conclusies uit de literatuurstudie. Content analyse richt zich op de manifeste betekenis en niet op de latente betekenis van de beschikbare data (Riffe et al., 2019). Hiermee is wel te beoordelen wat de organisatie zegt, maar niet wat de organisatie doet. Om dit nadeel te ondervangen zou aanvullend, kwalitatief onderzoek gedaan moeten worden. Hiervoor was de beschikbare tijd niet toereikend.

3.2. Technisch ontwerp: uitwerking van de methode

Onafhankelijke Variabele: Stakeholder Salience i.r.t. beveiliging persoonsgegevens en bescherming privacy

In het onderzoek is de onafhankelijke variabele Stakeholder Salience geoperationaliseerd door de prioriteit, die stakeholders geven aan de beveiliging van persoonsgegevens en bescherming van privacy (kortom Data Protection[4]) af te leiden uit de eerste dimensie van de materialiteitsmatrix. In bijlage 3a is deze afleiding verduidelijkt met een voorbeeld.

In het onderzoek zijn 2 onafhankelijke variabelen gemeten. Bij de eerste wordt de absolute mate van prioriteit van Data Protection voor stakeholders gemeten. Met deze variabele wordt hypothese 1 getoetst. Bij de tweede wordt de relatieve mate van prioriteit van Data Protection gemeten t.o.v. andere prioriteiten van stakeholders. Met deze variabele wordt hypothese 2 getoetst. Bij het beoordelen van de saillantie houden managers namelijk niet rekening met één stakeholder afzonderlijk, maar met verschillende stakeholders tegelijkertijd rekening (Griffin, 2017; Kuruppu et al., 2019; Mitchell et al., 2017; Neville et al., 2011).

O1 Absolute mate van Prioriteit van Data Protection voor Stakeholders
De absolute mate van prioriteit, die stakeholders (volgens de organisatie) geven aan Data Protection, blijkens de materialiteitsanalyse. Hierbij is de mate van prioriteit verdeeld in 5 gelijke, opeenvolgende klassen, variërend van 1 = laag tot en met 5 = hoog.

O2 Relatieve mate van Prioriteit van Data Protection voor Stakeholders
De relatieve mate van prioriteit, die stakeholders (volgens de organisatie) geven aan Data Protection t.o.v. andere onderwerpen, blijkens de materialiteitsanalyse. Hierbij is het gewogen aandeel bepaald volgens de formule:
absolute prioriteit Data Protection Stakeholders / [(aantal onderwerpen met prioriteit 1 x 1) + (aantal onderwerpen met prioriteit 2 x 2) + (aantal onderwerpen prioriteit 3 x 3) + (aantal onderwerpen prioriteit 4 x 4) + (aantal onderwerpen prioriteit 5 x 5)].

Afhankelijke Variabele: Symbolische versus Substantiële Legitimatie i.r.t. GDPR

In het onderzoek is de afhankelijke variabele 'symbolische versus substantiële legitimatie i.r.t. de GDPR' geoperationaliseerd door het totaal aantal GDPR-gerelateerde maatregelen, zoals deze tot uiting komen in de onderzochte publicaties van de beursgenoteerde ondernemingen. In totaal zijn er 24 verschillende maatregelen getoetst op aanwezigheid (ja = 1; nee =0). Deze maatregelen zijn benoemd in bijlage 3b. Hierbij is aangegeven op welk(e) artikel(en) in de GDPR de betreffende maatregel betrekking heeft. Al deze maatregelen hebben in beginsel een substantieel karakter, omdat deze de bedrijfsvoering op lange termijn beïnvloeden. Naarmate een organisatie een totaalscore heeft die dichter in de buurt komt van 24, wordt beoordeeld dat de organisatie een meer substantiële omgang heeft met de GDPR. Naarmate een organisatie een totaalscore heeft die dichter in de buurt komt van 0, wordt beoordeeld dat de organisatie een meer symbolische omgang heeft met de GDPR.

A Aantal GDPR gerelateerde maatregelen, variërend van 0 tot en met 24

Modererende Variabelen:

In het onderzoek zijn 2 modererende variabelen gemeten, die betrekking hebben op de beschikbare middelen. Met deze variabelen wordt hypothese 3 getoetst.

M1 Bedrijfsresultaat of Operating Income

[4] In de materialiteitsmatrices worden deze met elkaar samen hangende onderwerpen op verschillende manieren benoemd, namelijk als: Customer Privacy, Privacy Protection, Data Protection, Data Security, IT Security of Cyber Security. Al deze varianten zijn verzameld onder de term: Data Protection.

Wat is het bedrijfsresultaat of Operating Income van de organisatie volgens de onderzochte publicaties of eventuele andere openbare informatie?

M2 Omzet of Revenues / Net Sales
Wat is de omzet of Revenues / Net Sales van de organisatie volgens de onderzochte publicaties of eventuele andere openbare informatie?

Controle Variabelen:

In het onderzoek zijn 2 controle variabelen gemeten, die betrekking hebben op de tweede dimensie van de materialiteitsanalyse. Deze dimensie heeft betrekking op de mate van significantie, die de beveiliging van persoonsgegevens en bescherming van privacy heeft voor de waarde creatie van de organisatie. Deze variabelen zijn mogelijk ook van invloed of kunnen een verstorende effect hebben op de afhankelijke variabele c.q. op de verscheidenheid aan substantiële en symbolische legitimatie acties. De legitimatie acties die een organisatie onderneemt zijn namelijk niet alleen afhankelijk van de prioritering door stakeholders, maar ook van de significantie van dit onderwerp voor de missie en de strategie van de organisatie (Ashforth & Gibbs, 1990; Bundy et al., 2013; Bundy et al., 2018; Myllykangas et al., 2011).

C1 Absolute mate van Impact van Data Protection op de waarde creatie van de Organisatie
De absolute mate van impact, die Data Protection heeft op de missie/strategie van de organisatie, blijkens de materialiteitsanalyse. Hierbij is de mate van impact verdeeld in een 5-punts schaal, variërend van 1 = laag tot 5 = hoog.

C2 Relatieve mate van Impact van Data Protection op de waarde creatie van de Organisatie
De relatieve mate van belang, die Data Protection heeft t.o.v. andere onderwerpen op de missie/strategie van de organisatie, blijkens de materialiteitsanalyse. Hierbij is het gewogen aandeel bepaald volgens de formule:
absolute impact Data Protection / [(aantal onderwerpen met impact 1 x 1) + (aantal onderwerpen met impact 2 x 2) + (aantal onderwerpen met impact 3 x 3) + (aantal onderwerpen met impact 4 x 4) + (aantal onderwerpen met impact 5 x 5)].

In het onderzoek zijn daarnaast 3 controle variabelen gemeten, die mogelijk ook een verklarend effect kunnen hebben. Deze hebben betrekking op de onderkenning van de organisatie van het risico op datalekken of de bedreigingen en/of kansen i.r.t. cybercrime.

C3 Datalekken vormen een Risico voor de organisatie
Wordt door de organisatie expliciet beschreven, in de onderzochte publicaties, dat datalekken een risico kunnen vormen? 1 = expliciete beschrijving van risico, 0 = expliciete beschrijving van geen risico, blanco = geen expliciete beschrijving.

C4 Cybercrime vormt een Bedreiging voor de organisatie
Wordt door de organisatie expliciet beschreven, in de onderzochte publicaties, dat cybercrime een bedreiging kan vormen? 1 = expliciete beschrijving van bedreiging, 0 = expliciete beschrijving van geen bedreiging, blanco = geen expliciete beschrijving.

C5 Cybercrime vormt (ook) een Kans voor de organisatie
Wordt door de organisatie expliciet beschreven, in de onderzochte publicaties, dat cybercrime (ook) een kans kan vormen? 1 = expliciete beschrijving van kans, 0 = expliciete beschrijving van geen kans, blanco = geen expliciete beschrijving.

In het onderzoek is tenslotte een controle variabele gemeten, waarmee de organisaties onderling onderscheidbaar zijn.

C6 SIC code
In welke sector is de organisatie hoofdzakelijk actief, volgens de onderzochte publicaties of andere openbare informatie, conform Standard Industrial Classification (SIC)?

3.3. Gegevensanalyse

Om de mate van invloed te bepalen van de onafhankelijke variabele Stakeholder Salience i.r.t. Data Protection op de afhankelijke variabele 'substantiële versus symbolische omgang' i.r.t. de GDPR is een regressie analyse uitgevoerd, waarmee Hypothese 1 wordt getoetst. Hierbij wordt een lineair verband verondersteld, dat zich laat beschrijven in de volgende formule:

A (mate van substantiële omgang GDPR) =
β0 +
β1 x **O1 (absolute mate van Salience m.b.t. Data Protection)**

Hierbij is β1 de coëfficiënt, die het gewicht aangeeft van de variabele O1.

Op een vergelijkbare manier wordt Hypothese 2 getoetst. Hierbij wordt een lineair verband verondersteld, dat zich laat beschrijven in de volgende formule:

A (mate van substantiële omgang GDPR) =
β0 +
β1 x **O2 (relatieve mate van Salience m.b.t. Data Protection)**

Hierbij is β1 de coëfficiënt, die het gewicht aangeeft van de variabele O2.

Daarnaast is een regressie analyse uitgevoerd waarmee Hypothese 3 wordt getoetst. Hierbij wordt een lineair verband verondersteld, dat zich laat beschrijven in de volgende formule:

A (mate van substantiële omgang GDPR) =
β0 +
β1 x **O1 (mate van Salience m.b.t. Data Protection)** +
β2 x **M1 (mate van beschikbare middelen)** +
β3 x **MOD (mate van Salience x mate van beschikbare middelen)**

Hypothese 3 is ook nog op een vergelijkbare manier getoetst met variabele M2.

3.4. Waarborging validiteit, betrouwbaarheid en ethiek

Waarborging Interne Validiteit

De interne validiteit heeft betrekking op de mate waarin onderzoeksresultaten waarheidsgetrouw zijn en afhankelijk zijn van systematische interventies en niet van toevallige interpretaties van de onderzoeker (Saunders et al., 2016). In dit onderzoek gaat het dan voornamelijk om de kwaliteit van het meetinstrumentarium. Bij de operationalisatie en de meting van de onafhankelijke en afhankelijke variabelen is getracht zo veel mogelijk systematische fouten te voorkomen. Dit is hier onder toegelicht.

Operationalisatie en meting onafhankelijke variabele Stakeholder Salience:
In dit onderzoek wordt Stakeholder Salience als onafhankelijke variabele gebruikt, waarvan de waarde meetkundig wordt verkregen uit de materialiteitsanalyse c.q. materialiteitsmatrix van ondernemingen. Deze benadering is nieuw en de validiteit hiervan zal in verder onderzoek aangetoond moeten worden. Het voordeel van deze nieuwe benadering is echter dat deze minder complex en minder foutgevoelig is t.o.v. de benadering, waarbij Stakeholder Salience als een afhankelijke, samengestelde variabele wordt gebruikt, zoals in de benadering van Mitchell et al. (1997) en van diegenen die hierop postluderen en waarbij de waarden van de onderliggende elementen via taalkundige interpretaties vast gesteld moet worden. Wel moet opgemerkt worden dat er in dit onderzoek grensgevallen zijn, waarbij er gekozen moet worden of een waarde in de ene of andere categorie valt. Deze foutgevoeligheid is verkleind door een (binnen onderzoeken gangbare) 5-punts schaal te hanteren.

Operationalisatie en meting afhankelijke variabele Substantiële versus Symbolische Legitimatie:
In dit onderzoek wordt Substantiële versus Symbolische Legitimatie geoperationaliseerd door de uitkomst van de optelling van het al dan niet voorkomen van GDPR-gerelateerde maatregelen in de onderzochte publicaties. Omdat er geen ander vergelijkbaar onderzoek is dat als referentie kan dienen, is er door de onderzoeker zelf een instrumentarium ontwikkeld, gebaseerd op de verschillende artikelen uit de GDPR, waarmee de omgang met de GDPR gemeten wordt. De validiteit hiervan zal in verder onderzoek aangetoond moeten worden, maar doordat de meting betrekking heeft op 24 verschillende GDPR-gerelateerde maatregelen is deze zeer verfijnd. Wel moet opgemerkt worden dat het zo kan zijn dat een organisatie een maatregel wel beschrijft in hun publicaties, maar in werkelijkheid niet uitvoert of omgekeerd dat een organisatie een maatregel niet beschrijft in hun publicaties, maar in werkelijkheid wel uitvoert. Met deze vals positieven respectievelijk vals negatieven zouden dan verkeerde conclusies getrokken worden over de substantiële of symbolische omgang met de GDPR.

Binnen de beperkingen van dit onderzoek is deze foutgevoeligheid niet uit te sluiten, maar doordat in het onderzoek de data zijn van verzameld van een betrekkelijke grote hoeveelheid organisaties, die alle genoteerd staand op hoofdfondsen van Europese beurzen, zal deze foutgevoeligheid beperkt zijn.

Waarborging Externe Validiteit

De externe validiteit heeft betrekking op de mate waarin onderzoeksresultaten generaliseerbaar zijn voor alle relevante contexten (Saunders et al., 2016). Doordat de onderzoeksgegevens, waarop de onderzoeksresultaten gebaseerd zijn, van een betrekkelijk grote hoeveelheid verschillende organisaties afkomstig zijn, is het aannemelijk dat bij andere organisaties, die niet meegenomen zijn in dit onderzoek, vergelijkbare waarnemingen gedaan zouden kunnen worden. Hierbij moeten wel drie kanttekeningen geplaatst worden. Ten eerste kan er verschil ontstaan, doordat bij dit onderzoek gebruik is gemaakt van de publicaties van beursgenoteerde ondernemingen. De afwegingen die deze organisaties maken, over de mate waarin en wijze waarop onderwerpen gepubliceerd worden, kunnen verschillen t.o.v. ondernemingen uit de private sector, die niet beursgenoteerd zijn, maar ook t.o.v. organisaties in de publieke sector. Ten tweede kan er verschil ontstaan, doordat bij dit onderzoek gebruik is gemaakt van de verslaglegging van organisaties, die gebruik maken van de GRI-standaard. Deze organisaties kunnen naar een meer substantiële publicatie van hun beleid neigen dan organisaties, die geen gebruik maken van de GRI-standaard (Michelon et al., 2015; Perez-Batres et al., 2012). Ten derde kan er verschil ontstaan, doordat bij dit onderzoek gebruik is gemaakt van de verslaglegging van organisaties uit één jaar. Indien dit onderzoek in latere jaren herhaald zou worden, kunnen de onderzoekgegevens veranderen, omdat stakeholders hun prioriteiten kunnen aanpassen en omdat organisaties hun legitimatie acties kunnen aanpassen.

Waarborging Betrouwbaarheid

De betrouwbaarheid heeft betrekking op de mate waarin het onderzoek - het verzamelen en analyseren van de data - consistent en herhaalbaar is (Saunders et al., 2016). Dit vergt dat verschillende onderzoekers, die dezelfde methodologische regels toepassen, onafhankelijk van elkaar dezelfde bevindingen doen (Riffe et al., 2019). In dit onderzoek is dit op twee manieren ondervangen. Ten eerste door data te verzamelen uit stabiele, onveranderlijke bronnen, namelijk jaarverslagen en eventuele CSR rapportages, privacy statements/policies en codes of conduct/ethics, zoals deze in 2018 gepubliceerd zijn. Ten tweede door deze data zo eenduidig en eenvoudig mogelijk interpreteerbaar, codeerbaar en categoriseerbaar te maken. Hiervoor is een protocol opgesteld. Dit is toegelicht in bijlage 4. Ter verbetering van de betrouwbaarheid is bovendien gebruik gemaakt van een 2^{e} persoon, die een klein deel van de data ook heeft geïnterpreteerd, gecodeerd en gecategoriseerd. Hiermee is de betrouwbaarheid van het protocol getoetst. Daarnaast is de kwaliteit van de onderzoeksopzet en de onderzoeksresultaten beoordeeld door een academische begeleider en een academische meelezer.

Waarborging Ethiek

De ethiek heeft betrekking op de houding en het gedrag van de onderzoeker in relatie tot de rechten van diegenen, waarop het onderzoek van toepassing is en/of effect kan hebben. In dit onderzoek is dit ondervangen door transparant en integer te zijn in de methodes waarmee (publiekelijk verkrijgbare) onderzoeksgegevens geselecteerd en geanalyseerd zijn. Bovendien zijn de gemeten waarden traceerbaar gemaakt en, indien gewenst, raadpleegbaar voor anderen.

4. Resultaten

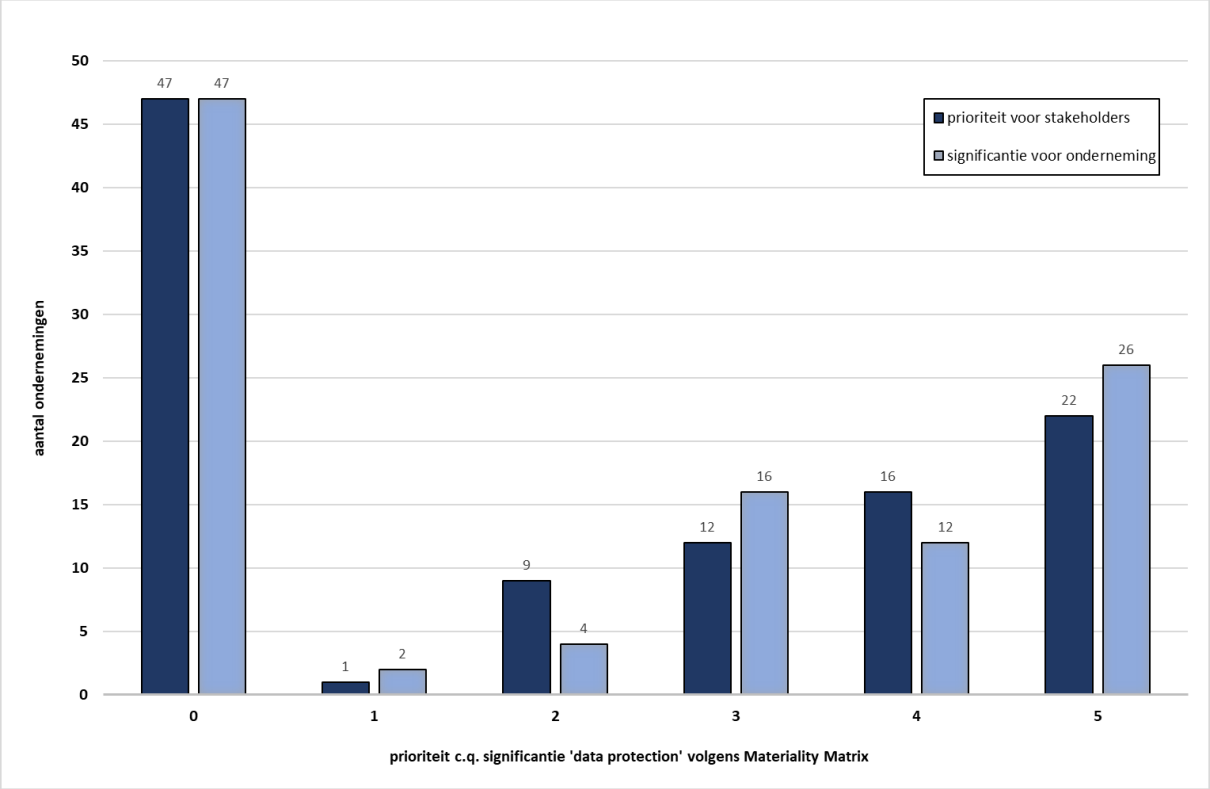
Van de 170 beursgenoteerde ondernemingen bleken er 107 de GRI-richtlijnen toe te passen én een materialiteitsmatrix opgenomen te hebben in hun jaarverslag c.q. CSR rapport. In de volgende paragrafen worden de resultaten van de data analyse behandeld.

4.1. Beschrijvende Statistiek

Saillantie Data Protection

Van de 107 onderzochte beursgenoteerde ondernemingen zijn er 47, die Data Protection (of een vergelijkbaar) onderwerp niet hebben opgenomen in hun Materiality Matrix. Bij 60 ondernemingen komt Data Protection wel terug als één van de onderwerpen. Bij 22 ondernemingen heeft Data Protection de hoogste saillantie d.w.z. heeft het hoogste prioriteit, die door stakeholders (in de perceptie van de onderneming) is toegekend. Bij 26 ondernemingen wordt aan Data Protection de hoogste significantie voor (de waarde creatie van) de onderneming toegekend. In figuur 6 is dit verder uitgewerkt.

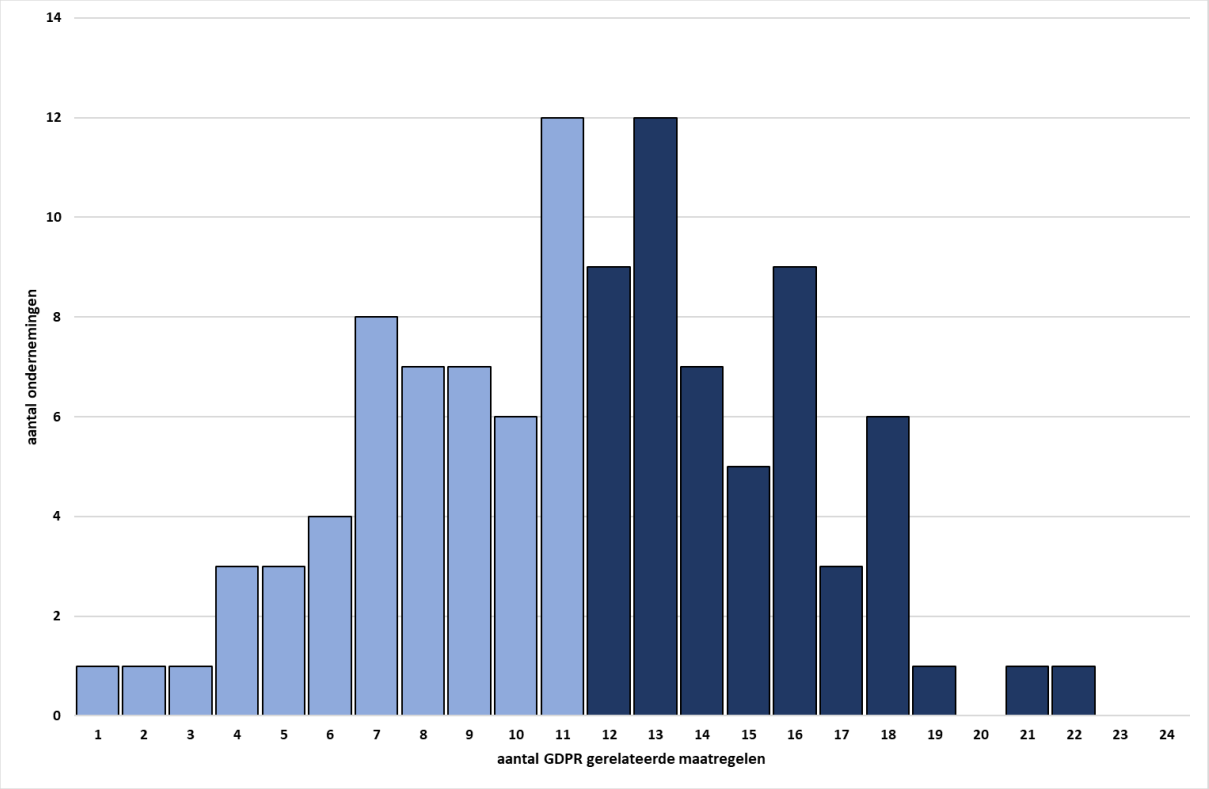
Figuur 6: saillantie van Data Protection voor stakeholders c.q. onderneming



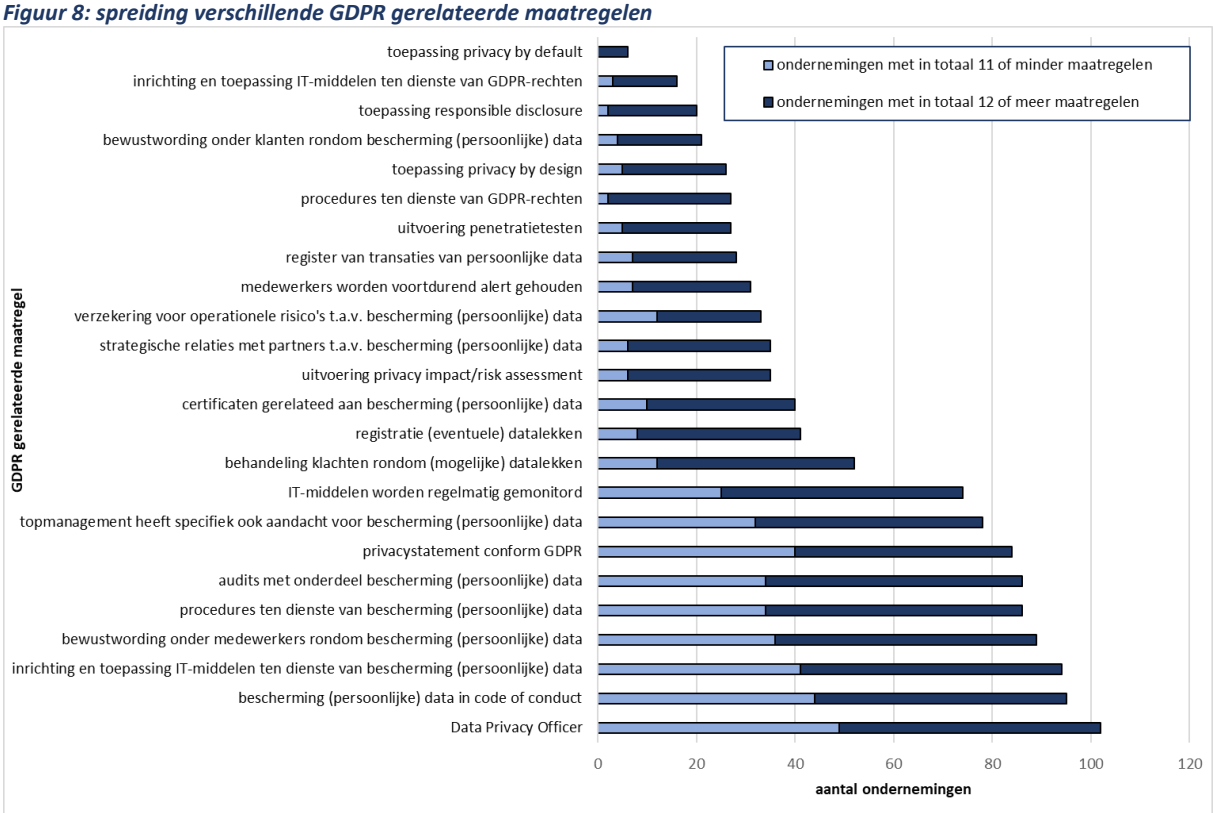
Omgang GDPR

Uit de content analyse van de publicaties van de onderzochte beursgenoteerde ondernemingen blijkt dat er een kopgroep is van 54 ondernemingen, die 12 of meer GDPR gerelateerde maatregelen hebben benoemd en dat er een groep van 53 achtervolgers is, die 11 of minder GDPR gerelateerde maatregelen hebben benoemd. De spreiding hiervan is weergegeven in figuur 7 en vertoont enige visuele kenmerken van een normale verdeling. Daarnaast is een analyse gemaakt van de mate waarin een GDPR gerelateerde maatregel voorkomt bij de onderzochte ondernemingen. De spreiding hiervan is weergegeven in figuur 8. De maatregel die het meest voorkomt (n= 102) is dat de onderneming een Data Protection Officer heeft, aansluitend bij artikelen 37, 38, en 39 van de GDPR. De maatregel die het minst voorkomt (n=6) is dat de onderneming de principes van 'privacy by default' toepast, aansluitend bij artikel 25 van de GDPR. De 6 ondernemingen, die deze maatregel benoemd hebben, maken deel uit van de kopgroep van ondernemingen, die 12 of meer GDPR gerelateerde maatregelen hebben benoemd. Uit de spreiding blijkt verder dat voor de top 9 van meest voorkomende maatregelen geldt dat de verschillen tussen de kopgroep en de groep achtervolgers nog betrekkelijk klein zijn, maar dat in de top 15 van minst voorkomende maatregelen de verschillen tussen de kopgroep en de groep achtervolgers betrekkelijk groot zijn.

Figuur 7: spreiding aantal GDPR gerelateerde maatregelen per onderneming



Figuur 8: spreiding verschillende GDPR gerelateerde maatregelen



Verschillen Sectoren

Van de 107 beursgenoteerde ondernemingen is op basis van de ICB classificatie een verdeling gemaakt naar de soort kernactiviteiten die zij verrichten. Tussen deze verschillende soorten ondernemingen zitten verschillen m.b.t. tussen de prioriteit die stakeholders aan Data Protection geven en het aantal GDPR-gerelateerde maatregelen. Ondernemingen in de sector 'Telecommunications' hebben de hoogste gemiddelde waarden. Ondernemingen in de sector 'Oil & Gas' hebben de laagste gemiddelde waarden. Dit is verder uitgewerkt in figuur 9.

Figuur 9: verschillen tussen sectoren

ICB Code	ICB Omschrijving	aantal ondernemingen	gemiddelde prioriteit stakeholders m.b.t. Data Protection	gemiddelde significantie ondernemingen m.b.t. Data Protection	gemiddeld aantal GDPR gerelateerde maatregelen
6000	**Telecommunications**	**5**	**4,6**	**4,6**	**18,2**
7000	**Utilities**	**5**	**1,6**	**1,8**	**15,6**
9000	**Technology**	**4**	**2,8**	**2,3**	**13,3**
8000	**Financials**	**26**	**3,1**	**3,0**	**13,1**
5000	**Consumer Services**	**10**	**1,7**	**2,3**	**12,9**
2000	**Industrials**	**21**	**2,2**	**2,0**	**11,3**
3000	**Consumer Goods**	**20**	**1,4**	**1,7**	**8,8**
1000	**Basic Materials**	**9**	**0,3**	**0,4**	**8,1**
4000	**Health Care**	**4**	**3,0**	**3,5**	**8,0**
0001	**Oil & Gas**	**3**	**0,0**	**0,0**	**5,3**
	TOTAAL	107	2,1	2,2	11,5

4.2. Univariate Analyse

Verkenning Variabelen; Correlatie

D.m.v. een (Pearson) correlatie analyse is onderzocht of er onderlinge lineaire verbanden bestaan tussen de verschillende variabelen. De resultaten van deze analyse zijn weergegeven in figuur 10.

Figuur 10: uitkomsten (Pearson) correlatie analyse

	Variabele	Gem.	Dev.	1	2	3	4	5	6	7	8	9	10
1	**aantal GDPR maatregelen**	11,460	4,250	1									
2	**absolute prioriteit stakeholders**	2,140	2,085	**,577****	1								
3	**gewogen prioriteit stakeholders**	0,039	0,044	**,576****	**,835****	1							
4	**absolute significantie onderneming**	2,210	2,136	**,539****	**,907****	**,763****	1						
5	**gewogen significantie onderneming**	0,037	0,042	**,552****	**,781****	**,921****	**,851****	1					
6	**datalekken is risico**	0,897	0,305	**,459****	**,216***	,182	**,235***	**,206***	1				
7	**cybercrime is bedreiging**	0,897	0,305	**,400****	**,245***	**,227***	**,264****	**,237***	**,291****	1			
8	**cybercrime is (ook) kans**	0,262	0,442	**,368****	**,421****	**,316****	**,373****	**,287****	,132	**,202***	1		
9	**bedrijfsresultaat x miljoen**	2711	2962	**,198***	**,209***	**,251****	**,249****	**,243***	,043	**,199***	,134	1	
10	**omzet x miljoen**	23788	26691	,169	,098	,027	,182	,069	,123	**,216***	**,191***	**,605****	1

* p < 0,05 (2-tailed); N=107

** p < 0,01 (2-tailed); N=107

Uit de correlatie analyse blijkt dat er tussen nagenoeg alle variabelen en 'aantal GDPR gerelateerde maatregelen' een significant verband bestaat, dat varieert van zwak tot redelijk sterk. Alleen tussen 'omzet' en 'aantal GDPR maatregelen' is geen significant verband aangetroffen. Dit betekent nog niet dat er een oorzakelijk verband is tussen deze correlerende variabelen. Dit zal moeten blijken uit de regressie analyse. Uit de correlatie analyse blijkt ook dat er tussen de meeste variabelen onderling significante verbanden bestaan, die variëren van zwak tot zeer sterk. Dit betekent dat er bij de regressie analyse getoetst moet worden op multicollineariteit. Dit betekent ook dat bij de regressie analyse getoetst moet worden of andere variabelen, behalve (absolute en gewogen) 'prioriteit stakeholders', mogelijk een verklarend of verstorend effect hebben op 'aantal GDPR gerelateerde maatregelen'.

4.3. Multivariate Analyse

Toetsing Hypothese 1; Regressie

D.m.v. een lineaire regressie is hypothese 1 getoetst. De resultaten van deze analyse zijn weergegeven in figuur 11.

Figuur 11: uitkomsten lineaire regressie Hypothese 1

Variabele	model H1.1	model H1.2	model H1.3	model H1.4	model H1.5	model H1.6
constante	**8,941****	**8,901****	**4,891****	**3,188****	**3,264****	**3,334****
absolute prioriteit stakeholders	**1,176****	**1,008****	**1,022****	**0,944****	**0,853****	
absolute significantie onderneming		0,181				
datalekken is risico			**4,881****	**4,189****	**4,160****	**4,904****
cybercrime is bedreiging				**2,776****	**2,616***	**3,386****
cybercrime is (ook) kans					1,103	**2,623****
***R*² gecorrigeerd**	0,327	0,322	0,440	0,470	0,476	0,340
F	**52,438****	**26,142****	**42,575****	**32,352****	**25,077****	**19,232****

afhankelijke variabele: aantal GDPR maatregelen

* p < 0,05

** p < 0,01

In model 1.1 is d.m.v. een enkelvoudige lineaire regressie analyse de hypothese getoetst m.b.t. het verklarende effect van Stakeholder Salience (geoperationaliseerd door 'absolute prioriteit stakeholders') op 'substantiële omgang met GDPR' (geoperationaliseerd door 'aantal GDPR maatregelen'). Hieruit blijkt dat 'absolute prioriteit stakeholders' een significant verklarend effect heeft op 'aantal GDPR maatregelen', $F(1,105) = 52,438$; $p < ,01$; $R^2 = ,327$.

In model 1.2 is getoetst of 'absolute significantie voor onderneming' een verstorend effect heeft door deze variabele aan model 1.1 toe te voegen. Uit de correlatie analyse blijkt namelijk dat significante verbanden bestaan tussen 'absolute significantie voor onderneming' en 'absolute prioriteit stakeholders' en tussen 'absolute significantie voor onderneming' en 'aantal GDPR maatregelen'. Hierdoor zou 'absolute significantie onderneming' een niet bestaand verband kunnen simuleren of een bestaand verband kunnen maskeren. Uit de meervoudige lineaire regressie blijkt echter dat deze variabele geen significant verklarend effect heeft ($p > ,05$) in het model en dus geen verstorend effect heeft.

In modellen 1.3 tot en met 1.6 is achtereenvolgens getoetst of de controle variabelen 'datalekken is risico', 'cybercrime is bedreiging', en 'cybercrime is (ook) kans' mogelijk ook een verklarend effect hebben. waarin de drie onafhankelijke variabelen alle significant zijn, $p < ,01$. In model 1.3 is behalve 'absolute prioriteit stakeholders' ook de variabele 'datalekken is risico' meegenomen. Dit model laat een significant verklarend effect zien, $F(2,104) = 42,575$; $p < ,01$; $R^2 = ,440$, waarin de beide onafhankelijke variabelen significant zijn, $p < ,01$. In model 2.4 is 'cybercrime is bedreiging' als extra onafhankelijke variabele meegenomen. Ook dit model laat een significant verklarend effect zien, $F(3,103) = 32,352$; $p < ,01$; $R^2 = ,470$, waarin alle drie de onafhankelijke

variabelen significant zijn, p < ,01. In model 1.5 is 'cybercrime is (ook) kans' als extra onafhankelijke variabele meegenomen. Ook dit model laat een significant verklarend effect zien, F(4,102) = 25,077; p < ,01; R^2 = ,476, maar hierin is de variabele 'cybercrime is kans' niet significant, p > ,05. In model 1.6 tenslotte is een meervoudige lineaire regressie uitgevoerd zonder de variabele 'absolute prioriteit stakeholders' en alleen met de 3 controle variabelen. Ook dit model laat een significant verklarend effect zien, F(3,103) = 19,232; p < ,01; R^2 = ,340, waarin alle variabelen significant zijn, p < ,01. Van de modellen 1.3 tot en met 1.6 is vastgesteld dat er geen multicollineariteit in het geding is (met VIF-waarden tussen 1 en 2). Uit de meervoudige lineaire regressies m.b.v. deze modellen blijkt dat 'absolute prioriteit stakeholders', maar ook de variabelen 'datalekken is risico' en 'cybercrime is bedreiging' een significant verklarend effect hebben op 'aantal GDPR maatregelen'.

Toetsing Hypothese 2; Regressie

D.m.v. een lineaire regressie is hypothese 2 getoetst. De resultaten van deze analyse zijn weergegeven in figuur 12.

Figuur 12: uitkomsten lineaire regressie Hypothese 2

Variabele	model H2.1	model H2.2	model H2.3	model H2.4	model H2.5
constante	**9,300****	**9,254****	**4,977****	**3,242****	**3,342****
gewogen prioriteit stakeholders	**55,179****	**42,788***	**48,809****	**45,333****	**41,191****
gewogen significantie onderneming		14,239			
datalekken is risico			**5,097****	**4,372****	**4,276****
cybercrime is bedreiging				**2,810****	**2,540***
cybercrime is (ook) kans					**1,490***
***R*² gecorrigeerd**	0,326	0,322	0,451	0,483	0,500
F	**52,198****	**26,201****	**44,572****	**33,996****	**27,475****

afhankelijke variabele: aantal GDPR maatregelen

* p < 0,05

** p < 0,01

In model 2.1 is d.m.v. een enkelvoudige lineaire regressie analyse de hypothese getoetst m.b.t. het verklarende effect van 'relatieve Stakeholder Salience' (geoperationaliseerd door 'gewogen prioriteit stakeholders') op 'substantiële omgang met GDPR' (geoperationaliseerd door 'aantal GDPR maatregelen). Hieruit blijkt dat 'gewogen prioriteit stakeholders' een significant verklarend effect heeft op 'aantal GDPR maatregelen', F(1,105) = 52,198; p < ,01; R^2 = ,326. Model 2.1 geeft met 32,6% dus een nagenoeg gelijke verklaring van de variantie in 'aantal GDPR maatregelen' als model 1.1 met 32,7%.

In de modellen 2.2 tot en met 2.5 zijn vergelijkbare stappen gemaakt als in de modellen 1.2 tot en met 1.5. Zo is in model 2.2 getoetst of 'gewogen significantie voor onderneming' een verstorend effect heeft, maar uit de meervoudige lineaire regressie blijkt dat deze variabele geen significant verklarend effect heeft (p > ,05). Zo is in modellen 2.3 tot en met 2.5 getoetst of de controle variabelen 'datalekken is risico', 'cybercrime is bedreiging', en 'cybercrime is (ook) kans', behalve 'gewogen prioriteit stakeholders', ook een verklarend effect hebben. In model 2.3 is behalve 'gewogen prioriteit stakeholders' ook de variabele 'datalekken is risico' meegenomen. Dit model laat een significant verklarend effect zien, F(2,104) = 44,572; p < ,01; R^2 = ,451, waarin de beide onafhankelijke variabelen significant zijn, p < ,01. In model 2.4 is 'cybercrime is bedreiging' als extra onafhankelijke variabele meegenomen. Ook dit model laat een significant verklarend effect zien, F(3,103) = 33,996; p < ,01; R^2 = ,483, waarin alle drie de onafhankelijke variabelen significant zijn, p < ,01. In model 2.5 is 'cybercrime is (ook) kans' als extra onafhankelijke variabele meegenomen. Ook dit model laat een significant verklarend effect zien, F(4,102) = 27,475; p < ,01; R^2 = ,500, waarin alle vier de onafhankelijke variabelen significant zijn, p < ,05. Van de modellen 2.3 tot en met 2.5 is vastgesteld dat er geen multicollineariteit in het geding is (met VIF-waarden tussen 1 en 2). De modellen 2.3 tot en met 2.5 geven een iets hogere verklaring van de variantie in 'aantal GDPR maatregelen' (respectievelijk 45,1%, 48,3% en 50,0%) dan de modellen 1.3 tot en

met 1.5 (respectievelijk 44,0%, 47,0% en 47,6%), maar de verschillen in robuustheid tussen deze verschillende modellen zijn betrekkelijk klein.

Toetsing Hypothese 3; Regressie

D.m.v. een lineaire regressie is hypothese 3 getoetst. De resultaten van deze analyse zijn weergegeven in figuur 13.

Figuur 13: uitkomsten lineaire regressie Hypothese 3

Variabele	model H3.1	model H3.2
constante	**11,137****	**11,046****
absolute prioriteit stakeholders gecentreerd	**0,835****	**1,055****
bedrijfsresultaat	0,000	
absolute prioriteit stakeholders gecentreerd X bedrijfsresultaat	**0,000***	
omzet		0,000
absolute prioriteit stakeholders gecentreerd X omzet		0,000
***R*² gecorrigeerd**	0,348	0,330
F	**19,884****	**18,426****

afhankelijke variabele: aantal GDPR maatregelen

* p < 0,05

** p < 0,01

In model 3.1 is de hypothese getoetst m.b.t. het modererende effect van 'bedrijfsresultaat' op de relatie tussen 'absolute prioriteit stakeholders' en 'aantal GDPR maatregelen'. Omdat de variabele 'absolute prioriteit stakeholders' waarde 0 kan hebben, is deze variabele eerst gecentreerd. Uit de meervoudige lineaire regressie analyse blijkt dat er een significant verklarend effect is, $F(3,103) = 19,884$; $p < ,01$; $R^2 = ,348$. Hierin is de variabele 'absolute prioriteit stakeholders gecentreerd x bedrijfsresultaat' significant, $p < ,05$, waardoor geconcludeerd kan worden dat 'bedrijfsresultaat' een modererend effect heeft. Hierbij moet overigens opgemerkt worden dat de regressiecoëfficiënt van deze variabele zeer klein is, < 0,001, maar dat deze variabele wel een belangrijk verklarend effect heeft, omdat de waarde van deze variabele zeer groot kan zijn.

In model 3.2 is getoetst of de controle variabelen 'omzet' ook een modererend effect heeft. Uit de meervoudige lineaire regressie analyse blijkt dat er een significant verklarend effect is, $F(3,103) = 18,426$; $p < ,01$; $R^2 = ,330$. Hierin is de variabele 'absolute prioriteit stakeholders gecentreerd x omzet' echter niet significant, $p > ,05$, waardoor geconcludeerd kan worden dat 'omzet' geen modererend effect heeft.

Van de modellen 3.1 en 3.2 is vastgesteld dat er geen multicollineariteit in het geding is (met VIF-waarden tussen 1 en 2).

5. Discussie

5.1. Conclusies

In de verschillende conclusies wordt ingegaan op de eerder gestelde hypothesen.

Conclusie Hypothese 1

Hypothese 1: Als stakeholders (in de perceptie van managers van een organisatie) een hoge (lage) absolute prioriteit geven aan Data Protection zal een organisatie een meer substantiële (symbolische) omgang hebben met de GDPR.

Uit de resultaten van de data analyse blijkt dat de mate van (absolute) Stakeholder Salience een significant verklarend effect heeft op symbolische versus substantiële legitimatie acties. Hoe lager de prioriteit die door stakeholders wordt toegekend aan Data Protection (in de perceptie van de organisatie), hoe meer symbolisch de legitimatieacties van de organisatie zijn i.r.t. de GDPR. Hoe hoger de prioriteit die door stakeholders wordt toegekend aan Data Protection (in de perceptie van de organisatie), hoe meer substantieel de legitimatieacties van de organisatie zijn i.r.t. de GDPR. Hypothese 1 wordt daarom aangenomen.

Conclusie Hypothese 2

Hypothese 2: Als stakeholders (in de perceptie van managers van een organisatie) een hoge (lage) relatieve prioriteit geven aan Data Protection t.o.v. andere onderwerpen zal een organisatie een meer substantiële (symbolische) omgang hebben met de GDPR.

Uit de resultaten van de data analyse blijkt dat de mate van relatieve Stakeholder Salience een significant verklarend effect heeft op symbolische versus substantiële legitimatie acties. Hoe lager de gewogen prioriteit die door stakeholders wordt toegekend aan Data Protection (in de perceptie van de organisatie), hoe meer symbolisch de legitimatieacties van de organisatie zijn i.r.t. de GDPR. Hoe hoger de gewogen prioriteit die door stakeholders wordt toegekend aan Data Protection (in de perceptie van de organisatie), hoe meer substantieel de legitimatieacties van de organisatie zijn i.r.t. de GDPR. Hypothese 2 wordt daarom aangenomen.

Conclusie Hypothese 3

Hypothese 3: Als een organisatie meer (minder) middelen ter beschikking heeft, dan zal dit een modererend effect hebben op een meer substantiële (symbolische) omgang met de GDPR.

Uit de resultaten van de data analyse blijkt dat het 'bedrijfsresultaat' een significant modererend effect heeft op de relatie tussen de saillantie van Data Protection en de omgang met de GDPR. Hoe meer middelen een organisatie beschikbaar heeft, hoe sterker het effect van de saillantie van Data Protection op de meer substantiële omgang met de GDPR. Hoe minder middelen een organisatie beschikbaar heeft, hoe sterker het effect op de meer symbolische omgang met de GDPR. Hypothese 3 wordt daarom aangenomen.

5.2. Reflecties

In verschillende reflecties wordt antwoord gegeven op de onderzoeksvragen. Daarnaast wordt gereflecteerd op andere bevindingen die in dit onderzoek zijn gedaan.

Reflectie 1; saillantie Data Protection voor stakeholders

Welke mate van prioriteit geven stakeholders - in de perceptie van organisaties - aan de beveiliging van persoonsgegevens en de bescherming van de privacy van burgers?

Dit onderzoek laat duidelijke verschillen zien in de prioriteit die stakeholders - in de perceptie van de onderzochte ondernemingen - geven aan Data Protection. De ondernemingen in de sectoren Telecommunications, Financials en Health Care percipiëren een hogere saillantie (gemiddeld 3 of hoger op een schaal van 5) dan de ondernemingen in de sectoren Oil & Gas, Basic Materials, Consumer Goods, Utilities en

Consumer Service (gemiddeld lager dan 2 op een schaal van 5). Uitgaande van de attributen van het (herziene) Stakeholder Salience model (zie figuur 2 en bijlage 2) kan dit duiden op gepercipieerde verschillen in de mate van macht die stakeholders uitoefenen, de mate van legitimiteit die stakeholders hebben, de mate van urgentie die stakeholders geven en de mate van nabijheid die stakeholders hebben. Hoewel dit verder niet onderzocht is, kunnen de verschillen in de saillantie van Data Protection mogelijk verklaard worden door:

- de omvang van de groepen stakeholders, waarvan persoonsgegevens door een onderneming worden verzameld/verwerkt (dit sluit aan op attribuut 'macht')
- de omvang van de persoonsgegevens van de groepen stakeholders, die door de onderneming worden verzameld/verwerkt (dit sluit aan op attribuut 'legitimatie')
- de mate van bedreiging voor de privacy voor stakeholders van deze transacties (dit sluit aan op attribuut 'urgentie') en
- de mate van waarneembaarheid van deze transacties voor stakeholders (dit sluit aan op attribuut 'nabijheid').

Reflectie 2; symbolische versus substantiële omgang GDPR

Welke mate van verscheidenheid tussen symbolische en substantiële legitimatie acties voeren organisaties uit bij hun omgang met de GDPR?

Dit onderzoek laat duidelijke verschillen zien tussen ondernemingen in de omgang met de GDPR. Dit komt tot uiting in de verschillen tussen het aantal GDPR gerelateerde maatregelen dat ondernemingen benoemen. Als dat aantal dichter in de buurt komt van 24, is beoordeeld dat de onderneming een meer substantiële omgang heeft met de GDPR. Als dat aantal dichter in de buurt komt van 0, is beoordeeld dat de onderneming een meer symbolische omgang met de GDPR heeft. Deze beoordeling is gebaseerd op een kwantitatief continuüm, waarbij wordt gevarieerd in de kwantiteit van de legitimatie acties. De ene helft van de ondernemingen heeft 12 of meer GDPR gerelateerde maatregelen genomen. Daaruit is af te leiden dat deze kopgroep een meer substantiële omgang met de GDPR heeft. De andere helft van de ondernemingen heeft 11 of minder GDPR gerelateerde maatregelen genomen. Daaruit is af te leiden dat deze groep achtervolgers een meer symbolische omgang met de GDPR heeft.

Een alternatieve benadering in dit onderzoek had kunnen zijn om de beoordeling te baseren op een kwalitatief continuüm, waarbij wordt gevarieerd in de kwaliteit van de legitimatie acties. Meer symbolische acties duiden dan op een symbolische benadering van de GDPR en meer substantiële acties duiden dan op een substantiële benadering van de GDPR. In dit onderzoek hebben alle geïnventariseerde legitimatie acties echter een substantieel karakter, omdat zij alle – in ieder geval in beginsel – gericht zijn op de bedrijfsvoering en op de lange termijn. Dit onderzoek laat tegelijkertijd opvallende verschillen zien in de mate waarin bepaalde GDPR gerelateerde maatregelen voor komen. Die verschillen zijn opvallend groot en roepen de vraag op of er tussen de verschillende GDPR gerelateerde maatregelen mogelijk toch sprake is van een kwalitatief continuüm. Daar wordt hierna verder bij stil gestaan.

Het is opvallend dat 95% van de ondernemingen een Data Protection Officer (DPO) heeft benoemd, aangezien deze benoeming waarschijnlijk niet voor alle in dit onderzoek bestudeerde ondernemingen verplicht is. Alleen voor ondernemingen, die op grote schaal of bijzondere persoonsgegevens verzamelen/verwerken, is dit verplicht (artikel 37 GDPR). Ook is het opvallend dat 89% van de ondernemingen de bescherming van (vertrouwelijke en/of persoonlijke) gegevens heeft opgenomen in een gedragscode, maar dat slechts 37% van de ondernemingen werkt met een certificaat, waarmee deze bescherming van gegevens getoetst is/wordt. Bovendien is het opvallend dat 80% van de ondernemingen beschrijft audits uit te voeren, waarin ook de bescherming van persoonsgegevens wordt beoordeeld en dat eveneens 80% van de ondernemingen beschrijft procedures te hebben, die de bescherming van persoonsgegevens ondersteunen, maar dat slechts 26% van de ondernemingen beschrijft een register te hebben, waarin de transactie van persoonsgegevens wordt gedocumenteerd (artikel 30 GDPR). Eveneens is het opvallend dat 79% van de ondernemingen een privacy statement/policy heeft, dat compliant is met de GDPR en waarin ook de omgang met de privacy rechten[5] van mensen is opgenomen, maar dat slechts 25% respectievelijk 15% van de ondernemingen beschrijft procedures/protocollen en IT-systemen geschikt te maken en te gebruiken voor het ondersteunen van deze privacy rechten van mensen. Hierbij is het ook opvallend dat slechts 24% respectievelijk 6% van de organisaties werkt volgens de principes van 'privacy by design' en 'privacy by default' (artikel 25 GDPR).

Hoewel dit verder niet onderzocht is, lijken de veel voorkomende maatregelen het minst ingrijpend te zijn. Deze kunnen daarmee een meer symbolisch karakter hebben. De maatregelen die betrekkelijk weinig voorkomen,

[5] Rechten op inzage, bezwaar, beperking, vergetelheid, mutatie, dataportabiliteit, toetsing en duidelijkheid.

lijken het meest ingrijpend te zijn en kunnen daarmee een meer substantieel karakter hebben. Dit onderzoek vormt echter een momentopname. Niet uit te sluiten is, dat naarmate de tijd vordert en ondernemingen meer mogelijkheden hebben gehad hun implementatie van de GDPR te evalueren en te verbeteren, dat GDPR gerelateerde maatregelen dan in kwantiteit en kwaliteit zullen toenemen. In die geleidelijkheid zouden maatregelen kunnen verschuiven van eerst voornamelijk een symbolisch karakter naar vervolgens een combinatie van een symbolisch én een substantieel karakter. Als hypothetisch voorbeeld van deze gedachtegang: in de organisatie, die (nog) geen gegevenstransactieregister heeft, heeft de DPO naar buiten toe een symbolisch karakter, maar naar binnen toe (nog) geen substantieel karakter, want zijn/haar toezichthoudende en adviserende rol heeft nog niet geleid tot de realisatie van het register; in de organisatie die wel een gegevenstransactieregister heeft, heeft de DPO naar buiten toe een symbolisch karakter, maar naar binnen toe ook een substantieel karakter. Met symbolische acties kunnen stakeholders op korte termijn tevreden gesteld worden, maar op lange termijn kunnen stakeholders alleen tevreden gesteld worden met substantiële acties (Berrone, Gelabert, & Fosfuri, 2009). Een geleidelijke verschuiving van eerst vooral alleen symbolische naar later ook substantiële acties, is in de veranderlijke context van IT mogelijk te verklaren, doordat de focus (van het IT management) van de organisatie niet alleen gericht moet zijn op het legitimeren van de bestaande, maar ook de toekomstige situatie (Magnusson & Bygstad, 2013) en niet alleen gericht moet zijn op het tegemoet komen aan bestaande behoeften, maar ook aan toekomstige behoeften van externe en interne stakeholders (Harguem et al., 2014). Met symbolische legitimatie acties kan nu legitimiteit verkregen worden, met een combinatie van symbolische én substantiële legitimatie acties kan voor de toekomst legitimiteit behouden worden.

Reflectie 3; verband tussen saillantie Data Protection en omgang met de GDPR

Wat is de invloed van de mate van Stakeholder Salience i.r.t. de beveiliging van persoonsgegevens en de bescherming van privacy op de mate van symbolische c.q. substantiële omgang met de GDPR door organisaties?

De GDPR, net zoals andere verordeningen, tracht de houding en het gedrag van mensen en organisaties te beïnvloeden, zodanig dat persoonsgegevens beveiligd zijn en de privacy van mensen beschermd wordt. Door hiertoe acties te nemen, kunnen organisaties op dit punt legitimiteit verkrijgen. Dit onderzoek bevestigt de theorie dat organisaties hierbij kiezen voor een mix van symbolische en substantiële legitimatie acties (Ashforth & Gibbs, 1990). Dit onderzoek bevestigt ook de aanwijzingen die er in de literatuur zijn gevonden (Bundy et al., 2013; Durand et al., 2019; Hyatt & Berente, 2017; Kuruppu et al., 2019; Perez-Batres et al., 2012; Schons & Steinmeier, 2016) dat deze keuze afhankelijk is van de mate van saillantie van een onderwerp – in dit geval de beveiliging van persoonsgegevens en de bescherming van privacy – voor een (groep) stakeholder(s). Dit onderzoek bevestigt ook de relevantie van Stakeholder Salience in de context van IT (Harguem et al., 2014) en het mitigeren van IT risico's en bedreigingen en het verkrijgen van legitimiteit van de stakeholders met betrekking tot IT gerelateerde onderwerpen (Haislip, Masli, Richardson, & Sanchez, 2016). Dit onderzoek bevestigt bovendien dat Stakeholder Theory en Legitimacy Theory met elkaar samenhangende theorieën zijn, die het CSR gedrag van organisaties kunnen verklaren. Met dit gedrag trachten organisaties niet alleen hun verantwoordelijkheid te demonstreren, maar trachten zij zich ook te conformeren aan maatschappelijke normen en verwachtingen en trachten zij hun onderneming te legitimeren (Fernando & Lawrence, 2014). Met dit gedrag trachten zij hun interne waardensystemen aan te laten sluiten op de externe waardesystemen van afzonderlijke stakeholders en de maatschappij als geheel (Chen & Roberts, 2010). Dit vergt investeringen en inspanningen en impliceert dat een organisatie niet in één keer, maar geleidelijk haar CSR gedrag - in dit geval t.a.v. de omgang met de GDPR - zal aanpassen. Dit onderzoek geeft aanleiding om te veronderstellen dat organisaties hierbij geleidelijk overgaan van alleen een symbolische omgang naar een combinatie van een symbolische én substantiële omgang met de GDPR. De mate van deze geleidelijkheid lijkt beïnvloed te worden door de mate van Stakeholder Salience m.b.t. Data Protection: hoe hoger de saillantie, hoe sneller de overgang. Dit is een hypothese die verder onderzocht zou moeten worden.

Reflectie 4; verschil tussen absolute en relatieve saillantie

Dit onderzoek laat geen duidelijke verschillen zien tussen het effect van absolute en relatieve Stakeholder Salience m.b.t. Data Protection op de omgang met de GDPR. Zou de determinatiecoëfficiënt in het model met relatieve Stakeholder Salience t.o.v. het model met absolute Stakeholder Salience lager zijn geweest, dan zou dit er op duiden dat het verklarend effect verzwakt wordt in combinatie met het toekennen van prioriteit aan andere claims. Dat zou in dit geval betekend hebben dat de claim t.a.v. data security / data privacy in verhouding minder bepalend is dan andere claims. Zou de determinatiecoëfficiënt in het model met relatieve Stakeholder Salience hoger zijn geweest, dan zou dit er op duiden dat het verklarend effect versterkt wordt in combinatie met het toekennen van prioriteit aan andere claims. Dat zou in dit geval betekend hebben dat de claim t.a.v. data security / data privacy in verhouding meer bepalend is dan andere claims. Nu dit verschil er niet is, lijkt een

substantiële omgang met de GDPR - onder invloed van een hoge saillantie van Data Protection - niet beïnvloed te worden door de hoge saillantie van andere onderwerpen. Dit duidt er op dat (managers van) organisaties niet alleen kunnen balanceren tussen verschillende onderwerpen met verschillende saillanties (Griffin, 2017; Kuruppu et al., 2019; Mitchell et al., 2017; Neville et al., 2011), maar ook tussen verschillende onderwerpen met dezelfde hoge mate van saillantie. Dit geeft extra inzicht in de wijze waarop organisaties omgaan met verschillende saillante stakeholders c.q. hun verschillende saillante claims en het responderen hierop met afzonderlijke legitimatieacties. Voor meer inzicht is verder onderzoek nodig.

Reflectie 5; andere invloeden op omgang met GDPR

Dit onderzoek maakt ook duidelijk dat er, behalve de saillantie van Data Protection, nog andere significante factoren zijn, die de omgang met de GDPR verklaren. Ondernemingen die datalekken als een risico onderkennen en die cybercrime als een bedreiging c.q. als een kans onderkennen nemen meer GDPR gerelateerde maatregelen dan ondernemingen die dit risico of deze bedreiging/kans niet onderkennen. Dit is op zichzelf niet verwonderlijk en lijkt te bevestigen dat de meer symbolische c.q. meer substantiële wijze waarop organisaties legitimatie acties nemen niet alleen afhankelijk is van de saillantie van een onderwerp voor stakeholders, maar ook van de significantie van dit onderwerp voor de missie en de strategie van de organisatie (Ashforth & Gibbs, 1990; Bundy et al., 2013; Bundy et al., 2018; Myllykangas et al., 2011). In dat verband is het echter opvallend dat de significantie van Data Protection voor de organisatie, weliswaar correleert met de saillantie voor de stakeholders, maar geen significant verklarend effect heeft op de omgang met de GDPR. Hiervoor is geen goede verklaring te geven binnen dit onderzoek.

Reflectie 6; modererend effect van beschikbare middelen

Dit onderzoek maakt duidelijk dat de mate van de beschikbare middelen c.q. de hoogte van het bedrijfsresultaat een modererend effect heeft op de invloed van de saillantie van Data Protection op de omgang met de GDPR. Dit bevestigt bevindingen uit eerder onderzoek dat hogere (c.q. lagere) beschikbare middelen te associëren zijn met meer substantiële (c.q. meer symbolische) strategische keuzen (Perez-Batres et al., 2012). Dit eerdere onderzoek gaat echter uit van een directe relatie tussen beschikbare middelen en de wijze waarop legitimatie acties worden genomen, terwijl dit onderzoek uit gaat van een indirecte relatie. Verder dient opgemerkt te worden dat het bedrijfsresultaat' slechts een indicatie vormt van de potentieel beschikbare middelen in een lopend jaar. Dit resultaat kan namelijk van jaar tot jaar verschillen. De kasstroom over een reeks van jaren zou een betere indicatie vormen.

5.3. Limitatie

De bevindingen in dit onderzoek zijn gebaseerd op gegevens uit openbare publicaties uit 2018 van 107 Europese beursgenoteerde ondernemingen, die een GRI standaard toepassen én een Materiality Matrix hebben opgenomen. Deze bevindingen hebben betrekking op de prioritering van Data Protection en de omgang met de GDPR. Dit impliceert dat dit onderzoek een aantal beperkingen heeft, namelijk:

- het aangetoonde significante verklarende effect van Stakeholder Salience m.b.t. Data Protection op de symbolische versus substantiële omgang met de GDPR is niet zonder meer te betrekken op niet-beursgenoteerde ondernemingen of op publieke organisaties of op andere CSR onderwerpen (zoals milieu vervuiling, corruptie, discriminatie, werkomstandigheden, e.d.)
- het aangetoonde niet significante effect van de saillantie van Data Protection voor de missie/strategie van de organisatie op de symbolische versus substantiële omgang met de GDPR is niet zonder meer te betrekken op niet-beursgenoteerde ondernemingen of op publieke organisaties of op andere CSR onderwerpen,
- het aangetoonde significante modererende effect van de grootte van het bedrijfsresultaat op de relatie tussen Stakeholder Salience m.b.t. Data Protection en de symbolische versus substantiële omgang met de GDPR is niet zonder meer te betrekken op niet-beursgenoteerde ondernemingen of op publieke organisaties of op andere CSR onderwerpen,
- de aangetoonde status van de omgang met de GDPR is niet zonder meer te betrekken op niet-beursgenoteerde ondernemingen of op publieke organisaties of op andere jaren dan 2018 en
- de aangetoonde status van de omgang met de GDPR is wel te betrekken op hetgeen de onderzochte ondernemingen gepubliceerd hebben, maar is niet zonder meer te betrekken op wat deze ondernemingen daadwerkelijk doen.

5.4. Aanbevelingen voor verder onderzoek

repliceren onderzoek voor andere CSR onderwerpen

In dit onderzoek is specifiek het effect bestudeerd van Stakeholder Salience m.b.t. Data Protection op de symbolische/substantiële omgang met de GDPR. Dit onderzoek zou gerepliceerd kunnen worden door andere CSR onderwerpen te bestuderen, zoals terugdringen van milieu emissies, tegen gaan van corruptie, tegen gaan van discriminatie, bevorderen werkomstandigheden, e.d. Op dezelfde manier zouden materialiteitsmatrices de bron kunnen vormen van de Stakeholder Salience m.b.t. dergelijke CSR onderwerpen. Op een vergelijkbare manier zouden openbare publicaties de bron kunnen vormen van de symbolische/substantiële omgang m.b.t. dergelijke CSR onderwerpen. Hiermee kan nog meer inzicht ontstaan in de invloed van Stakeholder Salience op de (symbolische/substantiële) legitimatie acties, die organisaties nemen om legitimiteit te verkrijgen/behouden van hun stakeholders m.b.t. deze CSR onderwerpen. Bij het repliceren van dit onderzoek zou ook het verschil tussen het effect van absolute en relatieve Stakeholder Salience verder onderzocht kunnen worden. Managers van organisaties houden namelijk rekening met verschillende saillante stakeholders en verschillende saillante onderwerpen tegelijkertijd (Griffin, 2017; Kuruppu et al., 2019; Mitchell et al., 2017; Neville et al., 2011). Hiermee zou meer inzicht kunnen ontstaan in het proces, waarmee managers balanceren tussen en responderen op deze verschillende stakeholders, hun verschillende claims en hun verschillende saillanties.

bestuderen Stakeholder Salience als variabele, die afgeleid is van Materiality Matrix en Analysis

In dit onderzoek is Stakeholder Salience als onafhankelijke variabele afgeleid van de materialiteitsmatrix. Hierdoor is er geen relatie gelegd met attributen, waarmee Stakehoder Salience in andere onderzoeken als afhankelijke variabele gedetermineerd werd. Het zou waardevol zijn om te onderzoeken of deze attributen/determinanten af te leiden zijn uit de materialiteitsanalyses, waarop organisaties hun materialiteitsmatrices hebben gebaseerd. Met een mix van kwantitatief en kwalitatief onderzoek zou hiermee gevalideerd kunnen worden dat Stakeholder Salience af te leiden is uit de materialiteitsmatrix. Bovendien zou het waardevol zijn om bij het bestuderen van de materialiteitsanalyses en -matrices Stakeholder Salience te verbinden met Stakeholder Work. Stakeholder Work omvat de doelgerichte processen, waarmee organisaties zich bewust zijn van hun stakeholders en stakeholders identificeren, begrijpen, prioriteren en betrekken (Mitchell et al., 2017). Het oorspronkelijke concept van Stakeholder Salience richtte zich vooral op het identificeren en prioriteren van stakeholders. Onderkend is dat het Stakeholder Salience concept aan kracht kan winnen door andere aspecten van Stakeholder Work hierin te integreren (Mitchell et al., 2017). Door op deze manier Stakeholder Salience te bestuderen, ontstaat verder inzicht in de relatie van Stakeholder Salience met het aspect betrekken van stakeholders en de relatie met het geven van informatie aan stakeholders en het nemen van (legitimatie) acties voor stakeholders.

onderzoeken effect Stakeholder Salience op lange termijn op de mix en intensiteit van legitimatie acties

Dit onderzoek is gestart vanuit de onderbouwing dat symbolische en substantiële legitimatie acties min of meer elkaars tegenovergestelden zijn. Ook in veel andere onderzoeken werden deze behandeld als ‘of/of’ fenomenen (Berrone et al., 2009). Toch zijn er aanwijzingen dat symbolische en substantiële legitimatie acties als ‘en/en’ fenomenen te beschouwen zijn en niet supplementair, maar complementair zijn (Berrone et al., 2009). Hierbij wordt het verschil tussen symbolische en substantiële legitimatie acties niet zo zeer bepaald door het verschil in karakter, zijnde oppervlakkig versus diepgaand, als wel door het verschil in doel, zijnde het beïnvloeden van de beeldvorming extern en het veranderen van de bedrijfsvoering intern. Het verschil tussen de intensiteit en mix van deze legitimatie acties lijkt daarbij vooral verklaard te worden door het effect dat organisaties er mee willen bereiken, namelijk het verkrijgen of behouden van legitimiteit (Ashforth & Gibbs, 1990). Dit onderzoek geeft hiervoor de volgende aanwijzingen:

- Voor het verkrijgen van legitimiteit lijkt voornamelijk de beeldvorming extern aangepakt te moeten worden.
- Voor het behouden van legitimiteit lijkt zowel de beeldvorming extern als de bedrijfsvoering intern (en daarmee ook de beeldvorming intern) aangepakt te moeten worden.
- Naarmate de saillantie van stakeholders en de saillantie van de claims die stakeholders op de organisaties leggen toeneemt, lijkt de intensiteit van deze legitimatie acties toe te moeten nemen.
- Naarmate deze saillantie afneemt, lijkt de intensiteit van deze legitimatie acties af te kunnen nemen.

Door middel van kwantitatief en kwalitatief longitudinaal onderzoek zouden deze afhankelijkheden en de variaties in mix en intensiteit verder bestudeerd kunnen worden.

onderzoeken wisselwerking tussen Stakeholder Salience en 'manager salience'

Onderwerpen, die saillant zijn voor stakeholders zijn daarmee voor organisaties relevant voor het verkrijgen en behouden van legitimiteit. Onderwerpen kunnen ook saillant zijn voor organisaties zelf voor het realiseren van hun missie en strategie (Ashforth & Gibbs, 1990; Bundy et al., 2013; Bundy et al., 2018; Myllykangas et al., 2011). Dit zou beschouwd kunnen worden als 'manager salience'. Als Stakeholder Salience gedefinieerd is als de mate, waarin managers van organisaties prioriteit geven aan de aanspraken die stakeholders op de organisatie maken, zou 'manager salience' te definiëren zijn als de mate, waarin managers van organisaties prioriteit geven aan de doelen die de organisatie wil bereiken. Zowel Stakeholder Salience als 'manager' salience zijn gebaseerd op de cognitie van de managers van een organisatie. Zowel Stakeholder Salience als 'manager' salience zijn van invloed bij het nemen van acties, die zich richten op de continuïteit van de organisatie. In dit onderzoek is op basis van de twee dimensies van de Materiality Matrix een correlatie vast gesteld tussen Stakeholder Salience en wat beschouwd kan worden als 'manager salience', maar er is geen significant verklarend effect vastgesteld van 'manager salience' op de wijze waarop legitimatie acties worden genomen. Door middel van kwantitatief en kwalitatief onderzoek zou meer inzicht kunnen ontstaan in de cognitie van managers - en de afwegingen die zij maken tussen de aanspraken die stakeholders willen maken en de doelen die de organisatie wil bereiken - en het nemen van legitimatie acties.

5.5. Aanbevelingen voor de praktijk

bundelen van legitimatie acties gericht op beeldvorming extern en bedrijfsvoering intern

Een tamelijk gangbare opvatting is dat organisaties legitimatie acties niet koppelen aan de interne bedrijfsvoering, omdat dit minder ingrijpend en daardoor minder kostbaar is. Door deze acties wel te koppelen aan de externe beeldvorming is de verwachting dat stakeholders toch voldoende tevreden gesteld kunnen worden, zodat organisaties toch legitimiteit verkrijgen van hun stakeholders (Fiss & Zajac, 2006). Er zijn echter aanwijzingen dat organisaties met deze symbolische benadering naar de toekomst toe risico's lopen t.g.v. toenemende kritiek en toenemende normatieve druk van stakeholders en extra (en daardoor ook meer kostbare) inspanningen moeten leveren om stakeholders tevreden te houden (Schons & Steinmeier, 2016). Er zijn ook aanwijzingen dat het los koppelen van de beeldvorming van de bedrijfsvoering niet alleen misleidend is voor externe stakeholders, maar ook voor interne stakeholders, waardoor deze onbewust ongewenst gedrag kunnen vertonen (MacLean & Behnam, 2010). Zodra de legitimiteit van een organisatie door stakeholders wordt betwijfeld, ontstaat het risico dat managers deze twijfels gaan bagatelliseren, betwisten of overaccentueren en zich gaan gedragen als 'clumsy', nervous' of 'overacting actors' (Ashforth & Gibbs, 1990). Managers van organisaties doen er daarom verstandig aan om legitimatie acties op lange termijn en afhankelijk van de saillantie van stakeholders niet alleen te richten op de beeldvorming extern, maar ook op de bedrijfsvoering intern en te acteren als 'balanced engagers' (Schons & Steinmeier, 2016). Hiermee kunnen deze organisaties een negatieve legitimatie spiraal voorkomen (Ashforth & Gibbs, 1990). Hiermee kunnen organisaties een betere positie in de markt innemen. Dit heeft mogelijk eerder positieve dan negatieve effecten op de financiële performance van een organisatie (Hyatt & Berente, 2017; Schons & Steinmeier, 2016). Dit pleit er daarom voor dat managers een combinatie van symbolische en substantiële legitimatie acties initiëren en wel koppelen aan de interne bedrijfsvoering.

toepassen GRI richtlijnen en werken aan stakeholders en legitimiteit

Het toepassen van de GRI richtlijnen, inclusief het maken van een materialiteitsanalyse en materialiteitsmatrix, maakt het mogelijk om op een gestructureerde manier informatie te geven aan stakeholders over de response van de organisatie op de voor stakeholders saillante onderwerpen. Door dit jaarlijks te doen en door hierbij ook de belangrijkste veranderingen te benoemen en te onderbouwen krijgen stakeholders kennis over de organisatie. Hiermee kan een organisatie niet alleen op een symbolische manier, maar ook op een meer substantiële manier invulling geven aan Stakeholder Work (Mitchell et al., 2017). Dit draagt bij aan het verkrijgen, behouden en mogelijk zelfs uitbreiden van legitimiteit en daarmee aan de continuïteit van de onderneming.

verder implementeren GDPR

Veel ondernemingen hebben een basis gelegd voor de verdere implementatie van de GDPR. Belangrijke maatregelen, die hiertoe veelal genomen zijn, zijn het benoemen van een DPO, het maken en publiceren van privacy beleid en privacy statements, het geven van trainingen aan medewerkers en het meenemen van gegevensbeveiliging als onderwerp in audits. Door alleen maatregelen te nemen, die een minder ingrijpend c.q.

een meer symbolisch karakter hebben, lopen ondernemingen het risico dat hun IT-security-investeringen en -inspanningen minder effectief zijn en uiteindelijk leiden tot meer datalekken en minder vertrouwen in de onderneming (Angst et al., 2017). Voor ondernemingen, die op grote schaal of bijzondere persoonsgegevens verzamelen/verwerken, verdient het aanbeveling kritisch te kijken of en hoe maatregelen zijn genomen t.a.v. de realisatie van het transactieregister van persoonsgegevens, de technische en organisatorische opvolging van de privacy rechten van mensen en de adoptie van 'privacy by design & default'. Voor het management van deze ondernemingen verdient het aanbeveling hier (onder supervisie van de DPO) specifiek op te sturen en toezicht op te houden. Op korte termijn kunnen dergelijke maatregelen misschien nog een disruptief karakter hebben en tekort schieten, maar door de leereffecten die hier mee gepaard gaan, zijn deze inspanningen op lange termijn meer effectief (Angst et al., 2017).

6. Dankwoord

Voor hun reflectie op mijn onderzoeksopzet en voor het op proef interpreteren, coderen en categoriseren van GDPR gerelateerde maatregelen uit een steekproef van jaarverslagen en CSR publicaties wil ik de heren R. Kronieger (crisismanager en GDPR-specialist) en J. Ramby (privacy- en security expert) danken. Voor zijn deskundige en motiverende begeleiding wil ik de heer L. Bollen (professor Informatie Management) danken. Door hen heb ik waardevolle input en inspiratie gekregen voor mijn scriptie. Bovendien wil ik mijn ouders danken voor hun belangstelling en steun. Bovenal wil ik mijn vrouw en kinderen danken, voor hun begrip – op de momenten dat mijn studie voor moest gaan – en voor hun aanmoediging (en soms ook aansporing) en hun vertrouwen. Door hen heb ik met nog meer voldoening aan mijn studie gewerkt en door hen rond ik mijn scriptie met nog meer trots af.

7. Literatuur

Angst, C. M., Block, E. S., D'Arcy, J., & Kelley, K. (2017). When do it security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches. *MIS Quarterly, 41*(3), 893-A898.

Ashforth, B. E., & Gibbs, B. W. (1990). The double-edge of organizational legitimation. *Organization Science, 1*(2), 177-194.

Berrone, P., Gelabert, L., & Fosfuri, A. (2009). The impact of symbolic and substantive actions on environmental legitimacy.

Bundy, J., Shropshire, C., & Buchholtz, A. K. (2013). Strategic cognition and issue salience: Toward an explanation of firm responsiveness to stakeholder concerns. *Academy of Management Review, 38*(3), 352-376.

Bundy, J., Vogel, R. M., & Zachary, M. A. (2018). Organization–stakeholder fit: A dynamic theory of cooperation, compromise, and conflict between an organization and its stakeholders. *Strategic Management Journal, 39*(2), 476-501. doi:10.1002/smj.2736

Chen, J. C., & Roberts, R. W. (2010). Toward a more coherent understanding of the organization–society relationship: A theoretical consideration for social and environmental accounting research. *Journal of Business Ethics, 97*(4), 651-665.

Cundill, G. J., Smart, P., & Wilson, H. N. (2018). Non-financial shareholder activism: A process model for influencing corporate environmental and social performance. *International Journal of Management Reviews, 20*(2), 606-626.

del Mar Alonso-Almeida, M., Llach, J., & Marimon, F. (2014). A closer look at the 'global reporting initiative' sustainability reporting as a tool to implement environmental and social policies: A worldwide sector analysis. *Corporate Social Responsibility and Environmental Management, 21*(6), 318-335.

Durand, R., Hawn, O., & Ioannou, I. (2019). Willing and able: A general model of organizational responses to normative pressures. *Academy of Management Review, 44*(2), 299-320.

Engelfriet, A., Chew-Meij, L., & Kager, P. (2018). *Handboek AVG Compliance in de praktijk (editie 2018)*. Amsterdam: Ius Mentis.

Fernando, S., & Lawrence, S. (2014). A theoretical framework for CSR practices: integrating legitimacy theory, stakeholder theory and institutional theory. *Journal of Theoretical Accounting Research, 10*(1), 149-178.

Fiss, P. C., & Zajac, E. J. (2006). The symbolic management of strategic change: Sensegiving via framing and decoupling. *Academy of Management Journal, 49*(6), 1173-1193. doi:10.5465/AMJ.2006.23478255

Freeman, R. E. (1984). *Strategic management : A stakeholder approach*. Marshfield, MA; University of Minnesota: Pitman ;.

Griffin, J. J. (2017). Tracing stakeholder terminology then and now: Convergence and new pathways. *Business Ethics: A European Review, 26*(4), 326-346.

Haislip, J. Z., Masli, A., Richardson, V. J., & Sanchez, J. M. (2016). Repairing organizational legitimacy following information technology (IT) material weaknesses: Executive turnover, IT expertise, and IT system upgrades. *Journal of Information Systems, 30*(1), 41-70.

Harguem, S., Karuranga, E., & Mellouli, S. (2014). *Examining the influence of external stakeholders on it governance: Perceptions of it executives.* Paper presented at the MCIS.

Hyatt, D. G., & Berente, N. (2017). Substantive or symbolic environmental strategies? Effects of external and internal normative stakeholder pressures. *Business Strategy and the Environment, 26*(8), 1212-1234.

Jawahar, I. M., & McLaughlin, G. L. (2001). Toward a descriptive stakeholder theory: An organizational life cycle approach. *The Academy of Management Review, 26*(3), 397-414.

Joos, H. C. (2019). Influences on managerial perceptions of stakeholder salience: two decades of research in review. *Management Review Quarterly, 69*(1), 3-37. doi:10.1007/s11301-018-0144-8

Khurram, S., Pestre, F., & Petit, S. C. (2019). Taking stock of the stakeholder salience tradition: Renewing the research agenda. *M@n@gement, 22*(2), 141-175.

Khurram, S., & Petit, S. C. (2017). Investigating the dynamics of stakeholder salience: What happens when the institutional change process unfolds? *Journal of Business Ethics, 143*(3), 485-515.
Kuruppu, S. C., Milne, M. J., & Tilt, C. A. (2019). Gaining, maintaining and repairing organisational legitimacy. *Accounting, Auditing & Accountability Journal*.
MacLean, T. L., & Behnam, M. (2010). The dangers of decoupling: The relationship between compliance programs, legitimacy perceptions, and institutionalized misconduct. *Academy of Management Journal, 53*(6), 1499-1520.
Magnusson, J., & Bygstad, B. (2013). Why I act differently: Studying patterns of legitimation among cios through motive talk. *Information Technology & People, 26*(3), 265-282.
Marimon, F., Alonso-Almeida, M. d. M., Rodríguez, M. d. P., & Cortez Alejandro, K. A. (2012). The worldwide diffusion of the global reporting initiative: What is the point? *Journal of Cleaner Production, 33*, 132-144.
Michelon, G., Pilonato, S., & Ricceri, F. (2015). Csr reporting practices and the quality of disclosure: An empirical analysis. *Critical Perspectives on Accounting, 33*, 59-78.
Mitchell, R. K., Agle, B. R., & Wood, D. J. (1997). Toward a theory of stakeholder identification and salience: Defining the principle of who and what really counts. *Academy of Management Review, 22*(4), 853-886.
Mitchell, R. K., Lee, J. H., & Agle, B. R. (2017). Stakeholder Prioritization Work: The Role of Stakeholder Salience in Stakeholder Research. In *Stakeholder Management* (Vol. 1, pp. 123-157): Emerald Publishing Limited.
Moratis, L., & Brandt, S. (2017). Corporate stakeholder responsiveness? Exploring the state and quality of gri-based stakeholder engagement disclosures of european firms. *Corporate Social Responsibility and Environmental Management, 24*(4), 312-325.
Myllykangas, P., Kujala, J., & Lehtimäki, H. (2011). Analyzing the essence of stakeholder relationships: What do we need in addition to power, legitimacy, and urgency? *Journal of Business Ethics, 96*(1), 65.
Neville, B. A., Bell, S. J., & Whitwell, G. J. (2011). Stakeholder salience revisited: Refining, redefining, and refueling an underdeveloped conceptual tool. *Journal of Business Ethics, 102*(3), 357-378.
Perez-Batres, L. A., Doh, J. P., Miller, V. V., & Pisani, M. J. (2012). Stakeholder pressures as determinants of csr strategic choice: Why do firms choose symbolic versus substantive self-regulatory codes of conduct? *Journal of Business Ethics, 110*(2), 157-172.
Riffe, D., Lacy, S., Fico, F., & Watson, B. (2019). *Analyzing media messages: Using quantitative content analysis in research*: Routledge.
Saunders, M., Lewis, P., & Thornhill, A. (2016). Research methods for business students (Vol. Seventh). *Harlow: Pearson Education*.
Schermer, B. W., Hagenauw, D., & Falot, N. (2018). Handleiding algemene verordening gegevensbescherming en uitvoeringswet algemene verordening gegevensbescherming.
Schons, L., & Steinmeier, M. (2016). Walk the talk? How symbolic and substantive csr actions affect firm performance depending on stakeholder proximity. *Corporate Social Responsibility and Environmental Management, 23*(6), 358-372.
Shabana, K. M., & Ravlin, E. C. (2016). Corporate social responsibility reporting as substantive and symbolic behavior: A multilevel theoretical analysis. *Business & Society Review (00453609), 121*(2), 297-327.
Teixeira, G. A., da Silva, M. M., & Pereira, R. (2019). The critical success factors of GDPR implementation: a systematic literature review. *Digital Policy, Regulation and Governance*.
Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review, 34*(1), 134-153.

Bijlage 1a: gedetailleerd overzicht literatuurstudie

Onderwerp	Zoeksleutels/-filters	Zoekmachine	Bronnen		
			Gevonden	Relevant	Geselecteerd
GDPR	'GDPR' or 'General Data Protection Regulation' + Full Text + Scholarly Journals	Ebsco Host	134	2	0
	Hintze, 2018; Wolters, 2018				
	'implementation GDPR' + Full Text + Scholarly Journals	Ebsco Host	3	0	0
	'compliance GDPR' + Full Text + Scholarly Journals	Ebsco Host	4	0	0
	'implementation GDPR'	Google Scholar	>200	3	**2**
	Politou et al., 2018; **Teixeira et al., 2019; Tikkinen-Piri et al., 2018**				
	'compliance GDPR'	Google Scholar	>200	3	**1**
	Politou et al., 2018; Presthus, 2018; **Tikkinen-Piri et al., 2018**				
Stakeholder Theory	Stakeholder Theory and 'overview or review or meta-analysis' + Full Text + Scholarly Journals	Ebsco Host	227	16	**6**
	Agle et al., 2008; **Bundy et al., 2013; Cundill et al., 2018;** Donaldson, 1999; Donaldson & Preston, 1995; Egels-Zandén & Sandberg, 2010; **Griffin, 2017; Jawahar & McLaughlin, 2001;** Jones, 1995; Jones et al., 2018; Jones & Wicks, 1999; **Khurram et al., 2019; Mitchell et al., 1997;** Richter & Dow, 2017; Sturdivant, 1979; Treviño & Weaver, 1999				
	Stakeholder Theory and 'IT Management'+ Full Text + Scholarly Journals	Ebsco Host	13	0	0
	Stakeholder Theory and 'regulation or law or policy or legislation'+ Full Text + Scholarly Journals	Ebsco Host	207	6	**1**
	Cragg, 2002; Desai, 2018; Egels-Zandén & Sandberg, 2010; **Griffin, 2017;** Jones, 1995; Kristin, 2015				
	Stakeholder Theory and 'GDPR'+ Full Text + Scholarly Journals	Ebsco Host	0	0	0
	Stakeholder Theory and 'data security' or Data Protection+ Full Text + Scholarly Journals	Ebsco Host	2	0	0
	'Stakeholder Management' and 'overview or review or meta-analysis'+ Full Text + Scholarly Journals	Ebsco Host	159	11	**1**
	Egels-Zandén & Sandberg, 2010; Escoubes, 1999; **Jawahar & McLaughlin, 2001;** Jones, 1995; Jones et al., 2018; Kracher & Martin, 2009; Post et al., 2002; Preble, 2005; Shah & Baskar, 2007; Sturdivant, 1979; Wood, 1991				
	'Stakeholder Management' and 'IT Management'+ Full Text + Scholarly Journals	Ebsco Host	38	0	0
	'Stakeholder Management' and 'regulation or law or policy or legislation'+ Full Text + Scholarly Journals	Ebsco Host	188	10	**1**
	Desai, 2018; Devinney et al., 2013; Egels-Zandén & Sandberg, 2010; Escoubes, 1999; **Griffin, 2017;** Harrison & St. John, 1996; Jones, 1995; Post et al., 2002; Vracheva & Mason, 2015; Wood, 1991				
	'Stakeholder Management' and 'GDPR'+ Full Text + Scholarly Journals	Ebsco Host	1	0	0
	'Stakeholder Management' and 'data security' or Data Protection+ Full Text + Scholarly Journals	Ebsco Host	3	0	0
Stakeholder Salience	Stakeholder Salience and 'overview or review or meta-analysis'+ Full Text + Scholarly Journals	Ebsco Host	11	5	**4**
	Bundy et al., 2013; Cundill et al., 2018; Jones et al., 2007; **Khurram et al., 2019; Mitchell et al., 1997**				
	Stakeholder Salience and 'IT Management'+ Full Text + Scholarly Journals	Ebsco Host	0	0	0

	Stakeholder Salience and 'IT Management'	Google Scholar	32	2	**1**
	De Vries et al., 2003; **Harguem et al., 2014**				
	Stakeholder Salience and 'regulation or law or policy or legislation'+ Full Text + Scholarly Journals	Ebsco Host	7	1	**1**
	Cundill et al., 2018				
	Stakeholder Salience and 'GDPR'+ Full Text + Scholarly Journals	Ebsco Host	0	0	0
	Stakeholder Salience and 'data security' or Data Protection+ Full Text + Scholarly Journals	Ebsco Host	0	0	0
	Stakeholder Salience and 'GDPR'	Google Scholar	5	0	0
	Stakeholder Salience and 'data security' or Data Protection	Google Scholar	37	0	0
Legitimacy Theory	Legitimacy Theory and 'overview or review or meta-analysis'+ Full Text + Scholarly Journals	Ebsco Host	48	4	**1**
	Bitektine & Haack, 2015; Frynas & Stephens, 2015; Michelon, 2011; **Shabana & Ravlin, 2016**				
	Legitimacy Theory and 'IT management'+ Full Text + Scholarly Journals	Ebsco Host	0	0	0
Symbolic versus Substantive Legitimacy	'Symbolic or Substantive' and 'Legitimacy'+ Full Text + Scholarly Journals	Ebsco Host	180	4	**2**
	Ashforth & Gibbs, 1990; Lightstone & Driscoll, 2008; Marquis & Qian, 2014; **Shabana & Ravlin, 2016**				
	'Symbolic Management' or 'Substantive Management'+ Full Text + Scholarly Journals	Ebsco Host	79	5	**2**
	Ashforth & Gibbs, 1990; Cundill et al., 2018; Fiss & Zajac, 2006; Johnson, 1990; Westphal & Zajac, 1998				
	'Symbolic or Substantive' and 'IT management' + Full Text + Scholarly Journals	Ebsco Host	2	0	0
	'Symbolic or Substantive' and 'Implementation or Adoption or Compliance'+ Full Text + Scholarly Journals	Ebsco Host	>200	3	**1**
	Angst et al., 2017; Lee, 2017; Mun, 2016				
Stakeholder Theory & Legitimacy Theory	Stakeholder Theory and Legitimacy Theory + Scholarly Journals	Ebsco Host	117	6	**1**
	Beske et al., 2020; **Chen & Roberts, 2010;** Desai, 2018; Fernando & Lawrence, 2014; Frynas & Stephens, 2015; **Shabana & Ravlin, 2016**				
Stakeholder Salience & Symbolic versus Substantive Legitimacy	Stakeholder Salience and 'Symbolic or Substantive'+ Full Text + Scholarly Journals	Ebsco Host	1	1	**1**
	Cundill et al., 2018				
verwijzingen naar '**Mitchell et al., 1997**' (n=13808)	Stakeholder Salience revisited	Google Scholar	>200	3	**3**
	Joos, 2019; Khurram et al., 2019; Mitchell et al., 2017				
	'Symbolic or Substantive'	Google Scholar	> 200	7	**6**
	Bundy et al., 2013; Bundy et al., 2018; Cundill et al., 2018; Durand et al., 2019; Mahon, 2002; **Myllykangas et al., 2011; Perez-Batres et al., 2012**				
	'IT Management'	Google Scholar	91	1	**1**
	Harguem et al., 2014				
verwijzingen naar '**Ashforth & Gibbs, 1990**' (n=2322)	Stakeholder Theory or Stakeholder Salience	Google Scholar	> 200	13	**8**
	Bundy et al., 2013; Chen & Roberts, 2010; Cundill et al., 2018; Frynas & Yamahaki, 2016; **Hyatt & Berente, 2017; Khurram et al, 2019; Khurram & Petit, 2017; Kuruppu et al., 2019**; Lightstone & Driscoll, 2008; MacLean & Benham, 2010; Mousa, 2010; **Neville et al., 2011; Schons & Steinmeier, 2016**				
	'IT Management'	Google Scholar	23	2	0
	Haislip et al., 2016; Magnusson & Bygstad, 2013				
CSR Disclosure	Corporate Social Responsibility and 'disclosure' + Full Text + Scholarly Journals	Ebsco Host	177	1	0

	Pollach, 2011				
	Corporate Social Responsibility and 'report' or 'reporting' + Full Text + Scholarly Journals	Ebsco Host	> 200	3	0
	Marquis & Qian, 2014; Peloza et al., 2012; Sehti et al., 2017				
	Corporate Social Responsibility and 'report' or 'reporting' and 'quality' + Full Text + Scholarly Journals	Ebsco Host	46	1	0
	Sehti et al., 2017				
	'Global Reporting Initiative' + Full Text + Scholarly Journals	Ebsco Host	88	2	0
	Calabrese et al., 2019; Sehti et al., 2017				
	'CSR Disclosure' and 'quality'	Google Scholar	>200	2	**1**
	Michelon et al., 2015; Sehti et al., 2017				
	'GRI' or 'Global Reporting Initiative' and 'quality'	Google Scholar	>200	6	**4**
	del Mar Alonso-Almeida et al., 2014; Fernandez-Feijoo et al., 2014; **Marimon et al., 2012; Michelon et al., 2015; Moratis & Brandt, 2017;** Sehti et al., 2017				

Bijlage 1b: gedetailleerd overzicht gevonden en geselecteerde artikelen

Relevante en Geselecteerde Bronnen	
Auteur(s), Jaartal	**Titel**
Agle et al., 2008	Dialogue: toward superior Stakeholder Theory.
Angst et al., 2017	**When do it security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches.**
Ashforth & Gibbs, 1990	**The double-edge of organizational legitimation.**
Beske et al., 2020	Materiality analysis in sustainability and integrated reports.
Bitektine & Haack, 2015	The "Macro" and the 'Micro"of legitimacy: toward a multilevel theory of the legitimacy process.
Bundy et al., 2013	**Strategic cognition and issue salience: toward an explanation of firm responsiveness to stakeholder concerns.**
Bundy et al., 2018	**Organization–stakeholder fit: A dynamic theory of cooperation, compromise, and conflict between an organization and its stakeholders.**
Calabrese et al., 2019	Materiality analysis in sustainability reporting: a tool for directing corporate sustainability towards emerging economic, environmental and social opportunities.
Cundill et al., 2018	**Non-financial shareholder activism: a process model for influencing corporate environmental and social performance.**
Chen & Roberts, 2010	**Toward a more coherent understanding of the organization–society relationship: a theoretical consideration for social and environmental accounting research.**
Cragg, 2002	Business ethics and Stakeholder Theory.
del Mar Alonso-Almeida et al., 2014	**A closer look at the 'global reporting initiative' sustainability reporting as a tool to implement environmental and social policies: A worldwide sector analysis.**
Desai, 2018	Collaborative stakeholder engagement: an integration between theories of organizational legitimacy and learning.
Devinney et al., 2013	A research agenda for global stakeholder strategy.
De Vries et al., 2003	Stakeholder identification in IT standardization processes.
Donaldson, 1999	Making Stakeholder Theory whole.
Donaldson & Preston, 1995	The Stakeholder Theory of the corporation: concepts, evidence, and implications.
Durand et al., 2019	**Willing and able: a general model of organizational responses to normative pressures.**
Egels-Zandén & Sandberg,	Distinctions in descriptive and instrumental Stakeholder Theory: a challenge for empirical research.
Escoubes, 1999	A framework for managing environmental strategy.
Fernandez-Feijoo et al., 2014	Effect of stakeholders' pressure on transparency of sustainability reports within the GRI framework.
Fernando & Lawrence, 2014	A theoretical framework for CSR practices: integrating Legitimacy Theory, Stakeholder Theory and institutional theory.
Fiss & Zajac, 2006	The symbolic management of strategic change: sensegiving via framing and decoupling.
Frynas & Stephens, 2015	Political Corporate Social Responsibility: reviewing theories and setting new agendas.
Frynas & Yamahaki, 2016	Corporate social responsibility: review and roadmap of theoretical perspectives.
Griffin, 2017	**Tracing stakeholder terminology then and now: convergence and new pathways.**
Haislip et al., 2016	Repairing organizational legitimacy following information technology (IT) material weaknesses: executive turnover, IT expertise, and IT system upgrades.
Harguem et al., 2014	**Examining the influence of external stakeholders on it governance: perceptions of it executives.**
Harrison & St. John, 1996	Managing and partnering with external stakeholders.
Hintze, 2018	Data Controllers, Data Processors and the growing use of connected products in the enterprise: managing risks, understanding benefits and complying with the GDPR.
Hyatt & Berente, 2017	**Substantive or symbolic environmental strategies? Effects of external and internal normative stakeholder pressures.**
Jawahar & McLaughlin, 2001	**Toward a descriptive Stakeholder Theory: an organizational life cycle approach.**
Johnson, 1990	Managing strategic change; the role of symbolic action.
Jones, 1995	Instrumental Stakeholder Theory: a synthesis of ethics and economics.
Jones et al., 2007	Ethical theory and stakeholder-related decisions: The role of stakeholder culture.
Jones et al., 2018	How applying instrumental Stakeholder Theory can provide sustainable competitive advantage.
Jones & Wicks, 1999	Convergent Stakeholder Theory.
Joos, 2019	**Influences onmanagerial perceptions of Stakeholder Salience: two decades of research in review.**
Khurram et al., 2019	**Taking stock of the Stakeholder Salience tradition: renewing the research agenda.**
Khurram & Petit, 2017	**Investigating the dynamics of Stakeholder Salience: What happens when the institutional change process unfolds?**
Kracher & Martin, 2009	A moral evaluation of online business protest tactics and implications for stakeholder management.
Kristin, 2015	Stakeholders theory- how they influence the business policy.
Kuruppu et al., 2019	**Gaining, maintaining and repairing organisational legitimacy.**
Lee, 2017	Why have policies often remained symbolic? Understanding the reasons for decoupling between policy and practice.
Lightstone & Driscoll, 2008	Disclosing elements of disclosure: a test of Legitimacy Theory and company ethics.
MacLean & Benham, 2010	The dangers of decoupling: The relationship between compliance programs, legitimacy perceptions, and institutionalized misconduct.
Magnusson & Bygstad, 2013	Why I act differently: studying patterns of legitimation among cios through motive talk.
Mahon, 2002	Corporate reputation: research agenda using strategy and stakeholder literature.
Marimon et al., 2012	**The worldwide diffusion of the global reporting initiative: What is the point?**
Marquis & Qian, 2014	Corporate social responsibility reporting in China: symbol or substance?

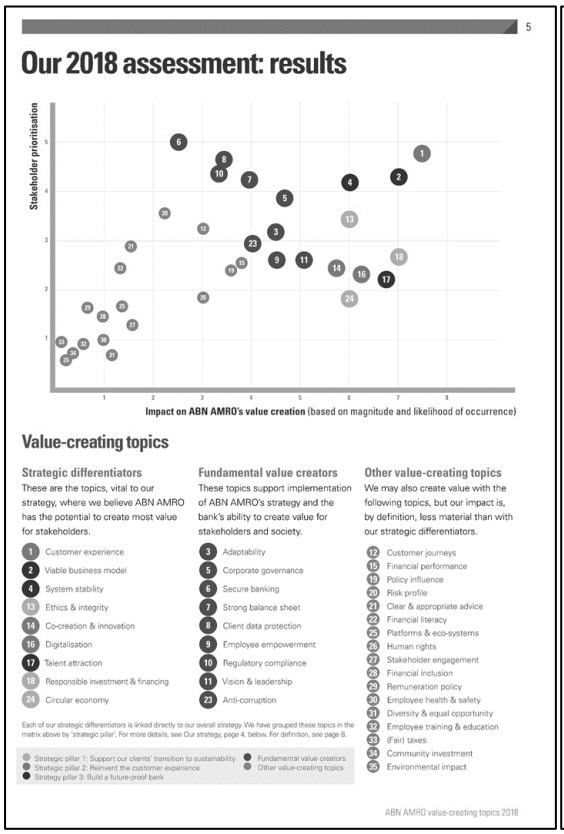
Michelon, 2011	Sustainability disclosure and reputation: a comparative study.
Michelon et al., 2015	**CSR reporting practices and the quality of disclosure: an empirical analysis.**
Mitchell et al., 1997	**Toward a theory of stakeholder identification and salience: Defining the principle of who and what really counts.**
Mitchell et al., 2017	**Stakeholder prioritization work: The role of Stakeholder Salience in stakeholder research.**
Moratis & Brandt, 2017	**Corporate stakeholder responsiveness? Exploring the state and quality of gri-based stakeholder engagement disclosures of european firms.**
Mousa, 2010	Stakeholder Theory as an arch to manage successful legitimacy strategies.
Mun, 2016	Negative compliance as an organizational response to legal pressures: the case of japanese equal employment opportunity law.
Myllykangas et al., 2011	**Analyzing the essence of stakeholder relationships: What do we need in addition to power, legitimacy, and urgency?**
Neville et al., 2011	**Stakeholder Salience revisited: refining, redefining, and refueling an underdeveloped conceptual tool.**
Peloza et al., 2012	Sustainability: how stakeholder perceptions differ from corporate reality.
Perez-Batres et al., 2012	**Stakeholder pressures as determinants of csr strategic choice: Why do firms choose symbolic versus substantive self-regulatory codes of conduct?**
Politou et al., 2018	Forgetting personal data and revoking consent under the GDPR: challenges and proposed solutions.
Pollach, 2011	Online privacy as a corporate social responsibility: an empirical study.
Post et al., 2002	Managing the extended enterprise: the new stakeholder view.
Preble, 2005	Toward a comprehensive model of stakeholder management.
Richter & Dow, 2017	Stakeholder Theory: A deliberative perspective.
Sehti et al., 2017	Enhancing the quality of reporting in corporate social responsibility guidance documents: the roles of iso 26000, global reporting initiative and csr-sustainability monitor.
Shabana & Ravlin, 2016	**Corporate social responsibility reporting as substantive and symbolic behavior: a multilevel theoretical analysis.**
Shah & Baskar, 2007	Corporate stakeholder management analysis tools: a review.
Schons & Steinmeier, 2016	**Walk the talk? How symbolic and substantive csr actions affect firm performance depending on stakeholder proximity.**
Sturdivant, 1979	Executives and activists: test of stakeholder management.
Teixeira et al., 2019	**The critical success factors of GDPR implementation: a systematic literature review.**
Presthus, 2018	GDPR compliance in Norwegian Companies.
Tikkinen-Piri et al., 2018	**EU General Data Protection Regulation: changes and implications for personal data collecting companies.**
Treviño & Weaver, 1999	The stakeholder research tradition: converging theorists + not convergent theory.
Vracheva & Mason, 2015	Creating firm value through stakeholder management and regulation.
Westphal & Zajac, 1998	The symbolic management of stockholders: corporate governance reforms and shareholder reactions.
Wolters, 2018	The control by and rights of the data subject under the GDPR.
Wood, 1991	Corporate social performance revisited.

Bijlage 2: Stakeholder Salience; oorspronkelijk en herzien construct

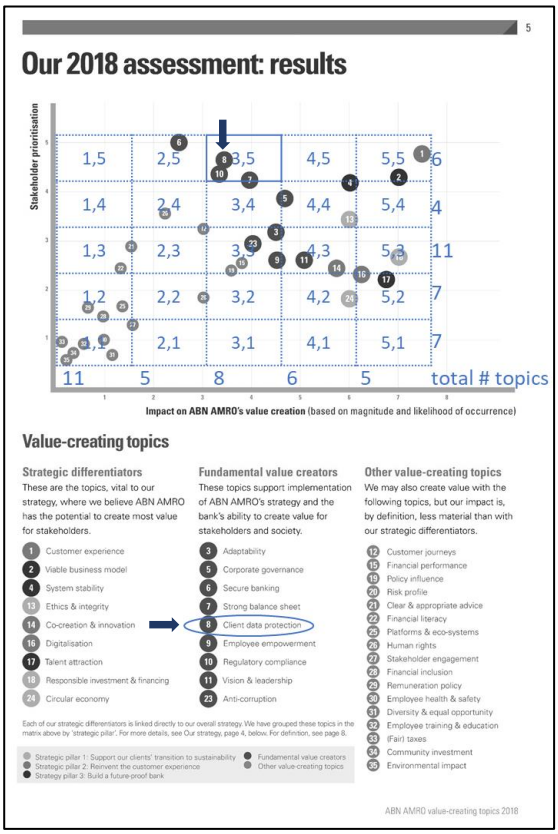
oorspronkelijk – Mitchell et al. 1997	herzien – Neville et al. 2011	herzien – Khurram & Petit 2017
Definitie: "The degree to which managers give priority to competing stakeholder claims."	**Definitie:** "The prioritization of stakeholder claims by managers based on their perception of the degree of power of the stakeholder and the degree of moral legitimacy and urgency of the claim."	**Definitie:** Idem als Mitchell et al. 1997
Attributen: • Power • Legitimacy • Urgency Een attribuut is aanwezig of niet, maar dit kan in de tijd veranderen.	**Attributen:** • Power (Stakeholder) • Moral Legitimacy (Claim) • Urgency (Claim) Een attribuut is gradueel aanwezig of niet en dit kan in de tijd veranderen.	**Attributen:** Als Mitchell et al. 1997, aangevuld met: • Proximity Een attribuut is aanwezig of niet, maar dit kan in de tijd veranderen.
Power (Macht): Het vermogen van actor A, waardoor actor B de outcome realiseert, die door actor A gewenst wordt. **Beginselen:** • Coercive Power; beïnvloeding door (fysieke) bedreiging of bestraffing • Utilitarian Power; beïnvloeding door (materiële) beloning • Normative Power; beïnvloeding door beroep te doen op sociaal geaccepteerde statussen en normen	**Power:** Idem als Mitchell et al. 1997	**Power (Macht):** Idem als Mitchell et al. 1997 **Beginselen:** Als Mitchell et al. 1997, aangevuld met: • Network Centrality; beïnvloeding door de centrale positie in het netwerk
Legitimacy (Legitimiteit): Een veronderstelling dat de acties van iets of iemand gewenst, gepast en geschikt zijn binnen een sociaal geconstrueerd stelsel van normen, waarden, overtuigingen en definities. **Beginselen:** • Institutional; Social Legitimacy • Organizational; Public Responsibility • Individual; Managerial Discretion	**Moral Legitimacy:** Een beoordeling van managers van de mate waarin de claim van een belanghebbende een grens overschrijdt van een individueel, organisatorisch of sociaal stelsel van normen, waarden, overtuigingen en defenties.	**Legitimacy:** Idem als Mitchell et al. 1997 **Beginselen:** • Moral: Consequential, Procedural, Structural/Categorical, Personal • Pragmatic: Exchange, Influence, Dispositional • Cognitive
Urgency (Urgentie): De mate waarin claims van belang-hebbenden vragen om onmiddellijke aandacht. **Beginselen:** • Time Sensitivity; de mate waarin een vertraging in de opvolging van de claim onacceptabel is voor de belanghebbende • Criticality; de mate waarin de claim of de relatie met organisatie belangrijk is voor de belanghebbende	**Urgency:** Er is een onderscheid tussen de belanghebbenden en de claims van belanghebbenden. Urgentie is een attribuut dat relevant is bij het prioriteren van claims van belanghebbenden, maar dat irrelevant is bij het identificeren van belang-hebbenden.	**Urgency:** Idem als Mitchell et al. 1997
		Proximity: Nabij zijn aan een belanghebbende in termen van ruimte, tijd of sociale hiërarchie. **Beginselen:** • Geographical Proximity; organisatie en belanghebbende zijn ruimtelijk nabij elkaar • Organised Proximity; organisatie en belanghebbende zijn maatschappelijk nabij elkaar door vergelijkbare praktijken, regels, normen, sociale codes, over-tuigingen en waarden

Bijlage 3a: Operationalisatie Stakeholder Salience i.r.t. Data Protection; uitwerking voorbeeld

Stap 1: selecteren materialiteitsanalyse



Stap 2: categoriseren waarden in 5 klassen



Stap 3: meten en berekenen waarden

- Variabele O.1: absolute prioriteit voor stakeholders = 5
- Variabele O.2: relatieve prioriteit voor stakeholders = 0,05 (=5,00%[6])
  = 5 / ((7*1) + (7*2) + (11*3) + (4*4) + (6*5))
- Variabele C.1: absolute impact organisatie = 3
- Variabele C.2: relatieve impact organisatie = 0,03 (=3,19%)
  = 3 / ((11*1) + (5*2) + (8*3) + (6*4) + (5*5))

[6] Ter vergelijking: als alle 35 onderwerpen even saillant zouden zijn, dan zou de relatieve prioriteit per onderwerp 1/35 = 2,86% bedragen.

Bijlage 3b: Operationalisatie ‘Symbolische versus Substantiële’ Legitimatie i.r.t. GDPR; 24 getoetste maatregelen

A.1 de organisatie heeft Data Protection/privacy opgenomen als thema of onderwerp in code of conduct / code of ethics / business principles / binding rules (artikelen 24, 40 en 47); ja = 1 / nee = 0 / onbekend = blanco

A.2 de organisatie heeft een privacystatement / privacypolicy uitgegeven conform GDPR (artikelen 12, 13, 14 en 24); ja = 1 / nee = 0 / onbekend = blanco

A.3 de organisatie gebruikt IT-middelen (infrastructuur/systemen/hardware/software), die de beveiliging/bescherming van informatie/data ondersteunen/waarborgen (artikelen 5, 9, 24 , 25 en 32); ja = 1 / nee = 0 / onbekend = blanco

A.4 de organisatie monitort de werking van deze IT-middelen regelmatig/voortdurend/pro-actief (artikelen 5, 9, 24 en 32); ja = 1 / nee = 0 / onbekend = blanco

A.5 de organisatie onderneemt penetratie-/intrusietesten/inbraaksimulaties/dataleksimulaties om de bescherming van informatie/data in de praktijk te toetsen (artikel 32); ja = 1 / nee = 0 / onbekend = blanco

A.6 de organisatie heeft een 'responsible disclosure' en biedt mogelijkheid om te 'ethical hacken' of biedt mogelijkheid om IT kwetsbaarheden te rapporteren (artikel 32); ja = 1 / nee = 0 / onbekend = blanco

A.7 de organisatie laat de privacy-/GDPR-rechten van subjecten (zoals recht op inzage, rectificatie of verwijdering) ondersteunen/waarborgen m.b.v. de IT-middelen (artikelen 12 tot en met 23); ja = 1 / nee = 0 / onbekend = blanco

A.8 de organisatie gebruikt procedures/protocollen/standaarden, die de beveiliging/bescherming van informatie/data ondersteunen/waarborgen (artikelen 5, 9, 24 , 25 en 32); ja = 1 / nee = 0 / onbekend = blanco

A.9 de organisatie laat de privacy-/GDPR-rechten van subjecten (zoals recht op inzage, rectificatie of verwijdering) ondersteunen/waarborgen m.b.v. procedures/protocollen/standaarden (artikelen 12 tot en met 23); ja = 1 / nee = 0 / onbekend = blanco

A.10 de organisatie heeft een register, waarin iedere transactie van persoonlijke gegevens wordt bijgehouden/gedocumenteerd (artikel 30); ja = 1 / nee = 0 / onbekend = blanco

A.11 de organisatie voert bij potentieel risicovolle verwerkingen van gegevens voorafgaand een risicoanalyse (privacy impact / risk assessment) uit (artikelen 35 en 36); ja = 1 / nee = 0 / onbekend = blanco

A.12 de organisatie registreert (eventuele) datalekken (artikelen 33 en 34); ja = 1 / nee = 0 / onbekend = blanco

A.13 de organisatie behandelt (eventuele) klachten rondom (mogelijke) datalekken (artikelen 33 en 34); ja = 1 / nee = 0 / onbekend = blanco

A.14 de organisatie past principes toe van privacy by default (artikel 25); ja = 1 / nee = 0 / onbekend = blanco

A.15 de organisatie past principes toe van privacy by design (artikel 25); ja = 1 / nee = 0 / onbekend = blanco

A.16 de organisatie heeft een Data Privacy/Security Officer/afdeling/team (artikelen 37, 38 en 39); ja = 1 / nee = 0 / onbekend = blanco

A.17 de organisatie geeft informatie aan en creëert bewustwording onder medewerkers (bijvoorbeeld door een instructie of een training) rondom data privacy/security (artikel 39); ja = 1 / nee = 0 / onbekend = blanco

A.18 de organisatie houdt medewerkers voortdurend alert (bijvoorbeeld: stuurt regelmatig pseudo phishing mails naar medewerkers / geeft regelmatig nieuws) (artikelen 5, 9, 24 , 25 en 32); ja = 1 / nee = 0 / onbekend = blanco

A.19 de organisatie geeft informatie aan en creëert bewustwording onder klanten rondom data privacy/security (artikelen 12, 13 en 14); ja = 1 / nee = 0 / onbekend = blanco

A.20 het topmanagement van de organisatie heeft specifiek ook aandacht voor data privacy/security/protection (bijvoorbeeld: heeft op agenda gestaan van bestuurlijk overleg, komt terug in functiegebieden, staat in 'letter CEO/COO') (artikelen 5, 9, 24 , 25 en 32); ja = 1 / nee = 0 / onbekend = blanco

A.21 de organisatie houdt audits waar beveiliging/bescherming informatie/data specifieke onderdelen van zijn (artikelen 5, 9, 24 , 25 en 32); ja = 1 / nee = 0 / onbekend = blanco

A.22 de organisatie heeft certificaten die gerelateerd zijn aan beveiliging/bescherming van informatie/data, zoals: ISO 21434, 22301, 27000, 27001, 27002, 31000 (artikelen 24 en 42); ja = 1 / nee = 0 / onbekend = blanco

A.23 de organisatie heeft een verzekering afgesloten voor operationele risico's/bedreigingen rondom beveiliging/bescherming informatie/data; ja = 1 / nee = 0 / onbekend = blanco

A.24 de organisatie onderhoudt strategische relaties met partners gericht op bevordering beveiliging/bescherming informatie/data (artikel 50); ja = 1 / nee = 0 / onbekend = blanco

Bijlage 4: protocol interpreteren, coderen en categoriseren gegevens

Onafhankelijke Variabele: Stakeholder Salience i.r.t. beveiliging persoonsgegevens en bescherming privacy

Bij het afleiden van de onafhankelijke variabele uit de materialiteitsmatrices zijn verschillende omschrijvingen van Material Topics geïncludeerd, die direct te relateren zijn aan de beveiliging van persoonsgegevens en de bescherming privacy. Dit zijn de termen: General Data Protection Regulation (GDPR), (Customer) Privacy, Privacy Protection, Data Protection, Data Security en IT Security. De term Cyber Security is hierbij ook meegerekend. Material Topics, die te algemeen zijn of niet direct te relateren zijn aan de beveiliging van persoonsgegevens en de bescherming van privacy beogen, zijn geëxcludeerd. Voorbeelden hiervan zijn: IT, Digital Technology, Digitisation, Digital Technology, Data Management, Data Science, Big Data, Human Rights, Safety, Business Ethics, Business Integrity, Business Continuity, Risk Management, Governance en Compliance.

Afhankelijke Variabele: Symbolische versus Substantiële Legitimatie i.r.t. GDPR

Bij het coderen van de afhankelijke variabele is eerst een 'sampling' doorgevoerd van de beschikbare content. Hierbij is in de content in eerste instantie gezocht op specifieke sleutelwoorden. Dit zijn: GDPR, Privacy, DPIA (Data Protection Impact Assessment), PIA (Privacy Impact Assessment), Data Protection, DPO (Data Protection Officer), Security Officer, Personal Data, Data Breaches, Data Security, IT Security, Cyber Security, Cyber Crime, Cyber Insurance, Network Security, Network Monitoring, Data Governance, Data Register, IT Governance, IT Risk(s), IT Vulnerabilities, IT Weaknesses, IT Monitoring, IT Audit(s), Responsible Disclosure, Ethical Hack(ing), ISO (27000, 27001, 27002, 21434, 22301, 31000) en Business Continuity[7]. Indien één van deze steekwoorden in een zin aangetroffen werd, werd deze zin als sample genomen en gearceerd. Indien twee of meer van deze steekwoorden in een alinea aangetroffen werden, werd deze hele alinea als sample genomen en gearceerd. Indien sleutelwoorden in twee of meer alinea's in een paragraaf aangetroffen werden, werd deze hele paragraaf als sample genomen en gearceerd. Zo ontstond voor iedere onderneming een set van samples, bestaande uit gearceerde zinnen, alinea's en paragrafen, die beoordeeld zijn op de aanwezigheid van de 24 vooraf gedefinieerde GDPR gerelateerde maatregelen. Bij 2 ondernemingen is getoetst of de sets van samples alle relevante content bevatten, die nodig is om de aanwezigheid van GDPR gerelateerde maatregelen te kunnen beoordelen. Dit bleek zo te zijn. Bij 5 ondernemingen is getoetst of een proefpersoon[8], op basis van dezelfde sets van samples uit de betreffende Jaarverslagen en CSR Rapporten van deze ondernemingen, dezelfde aanwezigheid scores noteerde t.a.v. de GDPR gerelateerde maatregelen als de onderzoeker. Dit bleek grotendeels zo te zijn. Alleen bij de maatregelen A.7 en A.9 noteerde de proefpersoon hogere aanwezigheid scores dan de onderzoeker. De beoordeling van de aanwezigheid van deze maatregelen lijkt gevoeliger te zijn voor interpretatieverschillen. Na zorgvuldige controle van de gearceerde (manifeste, niet latente) teksten kon de onderzoeker echter geen bevestiging vinden voor deze hogere scores en geen aanleiding vinden om de door de onderzoeker genoteerde scores, niet mee te nemen in de data analyse. De foutgevoeligheid m.b.t. deze maatregelen heeft een betrekkelijk gering effect op de uiteindelijke totale score van het aantal genoteerde GDPR maatregelen per onderzochte onderneming en de beoordeling van een meer symbolische dan wel meer substantiële omgang met de GDPR.

[7] Business Continuity is toegevoegd n.a.v. een advies van de 2 personen die op proef van 5 ondernemingen de samples beoordeeld hebben op de aanwezigheid van GDPR gerelateerde maatregelen.

[8] Initieel was hier ook een 2e proefpersoon bij betrokken, maar deze kon door persoonlijke omstandigheden de proef niet volledig afronden, waardoor de bevindingen van deze persoon verder niet zijn gebruikt.